

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    1 月 3 1 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 0 2 3 7 9 7  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 0 2 3 7 9 7 ]

出      願      人                      松下電器産業株式会社  
Applicant(s):

2 0 0 3 年    9 月 1 6 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 0 7 5 8 9 6

【書類名】 特許願

【整理番号】 2032740163

【提出日】 平成15年 1月31日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 辻 敦宏

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 横田 博史

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 五島 雪絵

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 高垣 景一

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

【代理人】

    【識別番号】 100097445

    【弁理士】

    【氏名又は名称】 岩橋 文雄

## 【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

## 【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

## 【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 暗号処理方法、および、暗号処理装置

【特許請求の範囲】

【請求項 1】 スケジュール部、暗号情報決定部、および、暗号処理部を備え、スケジュール部は、予約されるアプリケーションの予約登録と実行管理を行ない、

暗号情報決定部は、あらかじめ準備された複数の暗号アルゴリズムの選択を行ない、

暗号処理部は、準備された複数の暗号アルゴリズムのうち選択された暗号アルゴリズムの実行を行なう暗号処理方法であって、

スケジュール部は、スケジュール部に予約登録された、および、予約を要求された、暗号通信アプリケーションを含む複数のアプリケーション、および、準備された複数の暗号アルゴリズムのそれぞれに関して、それぞれが使用する使用資源の合計値を、複数の暗号アルゴリズム毎に算定し、

スケジュール部と暗号情報決定部は、使用資源合計値が許容資源使用量を越えない暗号アルゴリズムで、且つ、一定条件を満たす暗号アルゴリズムを選択し、

スケジュール部は、予約要求された暗号通信アプリケーションと、選択した暗号アルゴリズムとを、スケジュールに登録することを特徴とする暗号処理装置。

【請求項 2】 暗号通信アプリケーションの開始予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 3】 暗号アルゴリズムの使用開始予定時刻、あるいは、切換予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 4】 暗号通信用の鍵の寿命満了時刻以前の時間帯における（許容資源

使用量－使用資源合計値）に基づき、暗号通信用の更新鍵を生成するリキー処理の開示時刻を求め、リキー処理をスケジュールするようにし、リキー処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 5】前記使用資源の値について、その少なくともひとつは、予め設定された値、または、監視部により計測された値であることを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 6】前記使用資源の値について、その少なくともひとつは、監視部による計測に基づき初期設定された値、または、監視部により計測更新された値であることを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 7】複数の暗号アルゴリズムを選択し、途中で切り替えて使用するようにしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 8】暗号アルゴリズムを途中で切り替え、再び元の暗号アルゴリズムを使用する場合、暗号通信用の鍵を生成する前処理における生成結果を記憶しておき再利用するようにしたことを特徴とする請求項 7 に記載の暗号処理装置。

【請求項 9】前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、予約済み暗号通信アプリケーションおよび予約要求暗号通信アプリケーションに対して、必要なら前記一定条件にかかわらず、暗号アルゴリズムの再選択のための計算を行い、登録可能なら、再選択を実施して予約登録を行うことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 10】前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、他のアプリケーションの実行時間の変更、暗号通信平均データ転送量を低減する変更、もしくはこれに限らない変更を行い、必要なら前記一定条件にかかわらず、再選択を実施して予約登録を行うことを可能にしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 11】いずれかのアプリケーションの予約が取り消された場合、暗号通信アプリケーションの暗号アルゴリズムを再選択することを可能にしたことを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 12】前記変更、または、再選択を、予約要求元の指示に基づき行なうことを特徴とする請求項 9、10 または 11 に記載の暗号処理装置。

【請求項 13】使用資源合計値が許容資源使用量を越える場合、または、暗号アルゴリズムが選択できない場合、予約ができない旨の通知または表示を予約の要求元に対して行なうことを特徴とする請求項 1、9、10、11 のいずれか一項に記載の暗号処理装置。

【請求項 14】アプリケーションの予約を受け付け、仮にスケジュール登録する予約登録手順と、

受け付けたアプリケーションが、暗号アルゴリズムを使用するかどうかを判定し、暗号アルゴリズムを使用する場合は、それまでに受け付けている他のアプリケーションも含めて、各アプリケーションが使用する使用資源の量と、暗号アルゴリズムについては、複数用意されているそれぞれの暗号アルゴリズムについて使用資源の量とについて、暗号アルゴリズム毎に前記使用資源の合計値を算出する使用資源合計値算出手順と、

スケジュールのどの時点でも、使用資源合計値が許容資源使用量を越えることのない暗号アルゴリズムであって、所定の条件に合致する暗号アルゴリズムを選択する暗号アルゴリズム選択手順と、

受け付けたアプリケーションと選択した暗号アルゴリズムとをスケジュールに登録するスケジュール登録手順と、

を備えたことを特徴とする暗号処理方法。

【請求項 15】暗号通信アプリケーションの開始予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にする手順を有することを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 16】暗号アルゴリズムの使用開始予定時刻、あるいは、切替予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用

量以下にする手順を有することを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 17】暗号通信用の鍵の寿命満了時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の更新鍵を生成するリキー処理の開示時刻を求め、リキー処理をスケジュールするようにし、リキー処理を含めた使用資源の合計値を許容資源使用量以下にする手順を有することを特徴とする請求項 14 に記載の暗号処理装置。

【請求項 18】前記使用資源の値について、その少なくともひとつは、予め設定された値、または、監視手順により計測された値であることを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 19】前記使用資源の値について、その少なくともひとつは、監視手順による計測に基づき初期設定された値、または、監視手順により計測更新された値であることを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 20】複数の暗号アルゴリズムを選択し、途中で切り替えて使用するようにしたことを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 21】暗号アルゴリズムを途中で切り替え、再び元の暗号アルゴリズムを使用する場合、暗号通信用の鍵を生成する前処理における生成結果を記憶しておき再利用するようにしたことを特徴とする請求項 20 に記載の暗号処理方法。

【請求項 22】前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、予約済み暗号通信アプリケーションおよび予約要求暗号通信アプリケーションに対して、必要なら前記一定条件にかかわらず、暗号アルゴリズムの再選択のための計算を行い、登録可能なら、再選択を実施して予約登録を行うことを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 23】前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、他のアプリケーションの実行時間の変更、暗号通信平均データ転送量を低減する変更、もしくはこれに限らない変更を行い、必要なら前記一定条件にかかわらず、再選択を実施して予約登録を行うことを可能にしたことを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 24】いずれかのアプリケーションの予約が取り消された場合、暗号通信アプリケーションの暗号アルゴリズムを再選択することを可能にしたことを特徴とする請求項 14 に記載の暗号処理方法。

【請求項 25】前記変更、または、再選択を、予約要求元の指示に基づき行なうことを特徴とする請求項 22、23 または 24 に記載の暗号処理方法。

【請求項 26】使用資源合計値が許容資源使用量を越える場合、または、暗号アルゴリズムが選択できない場合、予約ができない旨の通知または表示を予約の要求元に対して行なうことを特徴とする請求項 14、22、23、24 のいずれか一項に記載の暗号処理方法。

【請求項 27】請求項 14～26 のいずれか 1 項に記載の方法を、コンピュータに機能させるためのプログラムとして記録した記録媒体。

【請求項 28】請求項 14～26 のいずれか 1 項に記載の方法を、コンピュータに機能させるためのプログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、暗号通信などのデータの通信を行う際に使用する暗号処理方法、および、暗号処理装置に関する。

##### 【0002】

##### 【従来の技術】

##### <ネット家電>

近年のインターネット技術の普及に伴い、携帯端末や家電製品などをインターネットに接続し、さまざまなサービスを展開しようという動きが活発になっている。インターネットに接続可能な家電製品のさきがけとして、現在 e p ステーションのような通信機能と録画機能が付いたデジタルテレビやセットトップボックスのような家電機器が発売されている。e p サービスの特徴は次の 2 つである。まず、放送局と e p ステーションをインターネットで結ぶことにより、放送と通信を融合したサービス、例えば TV ショッピングや視聴者参加型番組などを実現することができる。また、e p ステーションはハードディスクを備えるため、衛



星から放送されたTV番組や広告データ、インターネットから受信した電子メールデータなどを蓄積することができる。

#### 【0003】

現在のe pステーションでは、電話回線を用いてインターネットに接続している。しかし、ADSLやCATV、光ファイバーなどの高速回線の普及によって、家庭においても高速なインターネット接続環境が整いつつあり、今後高速通信が可能なe pステーションの後継機が登場することは容易に想像できる。

#### 【0004】

非特許文献1では、e pサービスの前身であるeプラットフォーム構想について述べられており、高画質放送とデータ放送、蓄積放送サービスやインターネットへの高速アクセスを連動させたサービスの形態が示されている。高速インターネットを利用したアプリケーションとしては、映像配信や音楽配信などのダウンロードサービス、テレビ電話やネットワークカメラによる監視などが考えられる。

#### 【0005】

これらの応用用途の中でネットワークカメラを利用する場合を考える。ネットワークカメラの民生用の利用法としては、保育所にいる子供の様子や、独居老人となっている親の様子、外出中の自宅の様子などを観察するなどが考えられる。このようなプライバシーを伴うような映像をインターネット上で盗み見られないようにするためには、映像データを暗号化などにより保護する必要がある。

#### 【0006】

暗号通信を必要とするものとしては、上記のような、プライベートなデータの送信、電子商取引に関するデータの送受信、インターネットサービスなどで、ISPから各顧客のシステムに対して行なう機器制御情報の伝送、携帯電話などの個人端末から自宅の端末装置に、留守の間に行なう操作情報の伝送、たとえば、風呂を沸かしたり、エアコンをONにしたりする、など、様々な用途がある。

#### 【0007】

##### <暗号通信>

従来から、機密性が必要とされるデータをインターネットなどの公衆ネットワ

ーク上でやりとりする場合には、データの暗号化処理が行われている。非特許文献2では、インターネット上に潜む危険と、その対策としての、暗号や認証の技術について詳しく述べられている。また、非特許文献3等には、インターネットで用いられている代表的な暗号化・認証プロトコルである、IPsec (Internet Protocol Security) について詳細に述べられている。

#### 【0008】

以下では、暗号通信の一般的な処理の流れを説明する。まず、双方において同じ暗号アルゴリズムを設定する。また、双方において、暗号化鍵と通信相手が暗号化したデータを復号化するための復号化鍵を設定する。暗号化鍵と復号化鍵が同じ場合は、共有鍵とも呼ばれる。なお、暗号アルゴリズムや鍵の設定は手動で設定するか、もしくは双方での間の自動ネゴシエーションによって行われる。以上の設定が完了すると、次のような手順で暗号通信が行われる。まず、データ送信側は、送信データを設定された暗号アルゴリズムと暗号化鍵を用いて暗号化し、インターネット回線網に送信する。受信側は、暗号化されたパケットを受信すると、設定された暗号アルゴリズムと復号化鍵を用いて、暗号化パケットを復号化する。

#### 【0009】

図9は、保育園に設置したネットワークカメラと家庭内のデジタルテレビをインターネット回線網で接続し、母親が、保育園での子供の状況を見ることができるようにしたシステムを想定した、暗号通信に関する部分を説明するブロック図である。

#### 【0010】

この場合、暗号処理部97は、デジタルテレビ自身の通信処理部96、インターネット回線網、相手のネットワークカメラの通信処理部86を介して、ネットワークカメラの暗号処理部87との間で、各種データをパケット形式にして通信を行なう。まず、データ送信側とデータ受信側が同じ暗号アルゴリズムを使用するために、双方の間で、上記のネゴシエーションが行われる。暗号アルゴリズムのネゴシエーションにおいては、ネゴシエーション用のパケットを、相手との間

でやり取りする。送信時には、暗号情報決定部 95 の指示に基づき、送信用のネゴシエーション packets を所定の形式で作成して、使用する暗号アルゴリズムを提案する。ネットワークカメラでは、通信処理部 86、暗号処理部 87 を経由して得た提案暗号アルゴリズムを暗号・復号情報として暗号情報決定部 85 に渡し、使用可能かどうかを暗号情報決定部 85 で判定する。そして、使用の可否を、暗号処理部 87、通信処理部 86 を経由して回答する。デジタルテレビの暗号情報決定部 95 は、回答を通信処理部 96、暗号処理部 97 を経由して受信し、受信した回答が、使用可能であれば、提案した使用可能な暗号アルゴリズムを確定することを、ネゴシエーション packets として、ネットワークカメラに通知して、使用する暗号アルゴリズムのネゴシエーションを終了する。また、暗号情報決定部 95 は、決定した暗号アルゴリズムを暗号処理部 97 に知らせて、アルゴリズム設定を指示する。また、暗号情報決定部 85 の方も、決定した暗号アルゴリズムを暗号処理部 87 に知らせて、アルゴリズム設定を指示する。その次に、暗号情報決定部 95、85、暗号処理部 87、87 は、お互いに所定の通信を行ない、設定した暗号アルゴリズムに従って決められた手順により、決められた形態の暗号化鍵や復号化鍵を作成、設定する。暗号化鍵や復号化鍵が生成されると、以降は、暗号通信が可能になる。暗号処理部 87 は、設定された暗号アルゴリズムを使用してカメラの映像データを暗号化し、データ packets 化して、通信処理部 86、インターネット回線網を経て、デジタルテレビに送る。デジタルテレビでは、データ packets を通信処理部 96 で受信し、暗号処理部 97 において、復号化し、復号化された映像データを暗号通信アプリケーション 93 に渡す。暗号通信アプリケーション 93 は、ネットワークカメラの映像データをテレビのディスプレイの所定位置に所定の大きさで表示する処理を行なう。

#### 【0011】

このような従来のネゴシエーションでは、暗号情報決定部 95 は、暗号アルゴリズムの提案を行なう場合には、保有している暗号アルゴリズムから、ユーザによって設定された、又はプログラム中であらかじめ定められている、ひとつ、または、複数の暗号アルゴリズムを選んで相手に提案する。また、相手から提案を受けた場合は、その提案に対する応答として、保有している暗号アルゴリズムの

中で最も高優先度の暗号アルゴリズムを選択し、通知するようにしている。

#### 【0012】

暗号通信アプリケーション 93、94 のように、暗号アルゴリズムにより、暗号化・復号化を行なう必要のあるアプリケーションが複数あり、複数種のデータを並行して暗号化・復号化処理を行なう場合、両方とも暗号強度の高いアルゴリズムを採用すると、一般的に、暗号アルゴリズムは、大きな CPU 処理能力を必要とするため、暗号通信アプリケーション 93、94 の処理と、それらのための複数の暗号処理全部を実行させると、CPU 処理能力を超えてしまい、システムが破綻する。このような事態を防ぐために、特許文献 1 では、通信データを複数のブロックに分割し、重要度の高いデータが格納されたブロックに対して、暗号強度が高い暗号アルゴリズムを使う一方、重要度の低いデータが格納されたブロックに対しては、暗号強度が低い暗号アルゴリズムを使うことにより、必要な CPU 処理資源量を逡減するようにしている。

#### 【0013】

##### 【非特許文献 1】

野村敦子著、「ブロードバンド革命—目指せ！ユビキタス・ネットワーク社会」、初版、中央経済社、平成 13 年 4 月 1 日、p. 225-227 (ISBN 4-502-57211-X)

##### 【非特許文献 2】

ユーリス・ブラック著、波多浩昭、松本直人訳、「インターネットセキュリティガイド」、初版、ピアソン・エデュケーション発行、2001 年 11 月 20 日、全頁 (ISBN 4-89471-455-8)

##### 【非特許文献 3】

「RFC 2401」、IETF (Internet Engineering Task Force) 発行

##### 【特許文献 1】

特開 2002-190798 号公報 (第 6 頁、第 6 図)

#### 【0014】

##### 【発明が解決しようとする課題】

上述したように、暗号通信で行われる暗号処理は、送受信データに対して複雑な処理を行う必要がある。このため、暗号通信は、暗号化を行わない通信に比べて、非常に処理負荷が高くなる。たとえば、ネットワークカメラデータの復号化処理（暗号通信アプリケーション 93）と、テレビ放送の映像データの録画（アプリケーション 91）という、リアルタイムに処理しなければならない高負荷な処理が重なった場合、前述のようなネゴシエーションでは、より暗号強度が高い暗号アルゴリズムを選択するので、内蔵 CPU の処理能力では、両方を同時には処理しきれない可能性がある。つまり、TV 放送の録画に失敗するか、もしくは、ネットワークカメラの画像が乱れたり止まったりするという問題が発生することがある。また、重要度の高いデータを扱う暗号通信に対して、暗号強度が高い暗号アルゴリズムを使い、重要度の低いデータを扱う暗号通信に対して、暗号強度が低い暗号アルゴリズムを使うことにより、必要な CPU 処理資源量を逡減するようにしても、やはり、全部を処理しきれない可能性がある。

#### 【0015】

本発明の目的は、暗号通信処理と他の高負荷な処理を同時に行わなければならない場合に、できるだけ強固な機密性を提供しつつも、暗号処理の負荷を軽減し、CPU リソースの枯渇によって生じる上記のような問題を解決する方法を提供することである。

#### 【0016】

##### 【課題を解決するための手段】

上記課題を解決するために、本発明の暗号処理装置、および、暗号処理方法は、以下のようにする。

#### 【0017】

(1) スケジュール部、暗号情報決定部、および、暗号処理部を備え、スケジュール部は、予約されるアプリケーションの予約登録と実行管理を行ない、暗号情報決定部は、あらかじめ準備された複数の暗号アルゴリズムの選択を行ない、暗号処理部は、準備された複数の暗号アルゴリズムのうち選択された暗号アルゴリズムの実行を行なう暗号処理方法であって、スケジュール部は、スケジュール部に予約登録された、および、予約を要求された、暗号通信アプリケーションを

含む複数のアプリケーション、および、準備された複数の暗号アルゴリズムのそれぞれに関して、それぞれが使用する使用資源の合計値を、複数の暗号アルゴリズム毎に算定し、スケジュール部と暗号情報決定部は、使用資源合計値が許容資源使用量を越えない暗号アルゴリズムで、且つ、一定条件を満たす暗号アルゴリズムを選択し、スケジュール部は、予約要求された暗号通信アプリケーションと、選択した暗号アルゴリズムとを、スケジュールに登録することを特徴とする暗号処理装置、あるいは、方法とする。

#### 【0018】

(2) 暗号通信アプリケーションの開始予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする（1）に記載の暗号処理装置、あるいは、方法とする。

#### 【0019】

(3) 暗号アルゴリズムの使用開始予定時刻、あるいは、切換予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする（1）に記載の暗号処理装置、あるいは、方法とする。

#### 【0020】

(4) 暗号通信用の鍵の寿命満了時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の更新鍵を生成するリキー処理の開示時刻を求め、リキー処理をスケジュールするようにし、リキー処理を含めた使用資源の合計値を許容資源使用量以下にしたことを特徴とする（1）に記載の暗号処理装置、あるいは、方法とする。

#### 【0021】

(5) 前記使用資源の値について、その少なくともひとつは、予め設定された値、または、監視部により計測された値であることを特徴とする（1）に記載の暗号処理装置、あるいは、方法とする。

**【0022】**

(6) 前記使用資源の値について、その少なくともひとつは、監視部による計測に基づき初期設定された値、または、監視部により計測更新された値であることを特徴とする (1) に記載の暗号処理装置、あるいは、方法とする。

**【0023】**

(7) 複数の暗号アルゴリズムを選択し、途中で切り替えて使用するようにしたことを特徴とする (1) に記載の暗号処理装置、あるいは、方法とする。

**【0024】**

(8) 暗号アルゴリズムを途中で切り替え、再び元の暗号アルゴリズムを使用する場合、暗号通信用の鍵を生成する前処理における生成結果を記憶しておき再利用するようにしたことを特徴とする (7) に記載の暗号処理装置、あるいは、方法とする。

**【0025】**

(9) 前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、予約済み暗号通信アプリケーションおよび予約要求暗号通信アプリケーションに対して、必要なら前記一定条件にかかわらず、暗号アルゴリズムの再選択のための計算を行い、登録可能なら、再選択を実施して予約登録を行うことを特徴とする (1) に記載の暗号処理装置、あるいは、方法とする。これは、予約済みの暗号通信アプリケーション用の暗号アルゴリズムが、前記一定条件を満たす暗号強度の中で強度が上位のものを採用している場合、一定条件はそのままでも、その条件下で、より暗号強度が低位のものに変更する操作を含む。また、このような変更の余地がない場合は、前記一定条件を緩和することを含む。

**【0026】**

(10) 前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、他のアプリケーションの実行時間を変更する、暗号通信平均データ転送量を低減するなどの変更、もしくはこれに限らない変更を行い、必要なら前記一定条件にかかわらず、再選択を実施して予約登録を行うことを可能にしたことを特徴とする (1) に記載の暗号処理装置、あ

るいは、方法とする。

**【0027】**

(11) いずれかのアプリケーションの予約が取り消された場合、暗号通信アプリケーションの暗号アルゴリズムを再選択することを可能にしたことを特徴とする(1)に記載の暗号処理装置、あるいは、方法とする。

**【0028】**

(12) 前記変更、または、再選択を、予約要求元の指示に基づき行なうことを特徴とする(9)、(10)、(11)に記載の暗号処理装置、あるいは、方法とする。

**【0029】**

(13) 使用資源合計値が許容資源使用量を越える場合、または、暗号アルゴリズムが選択できない場合、予約ができない旨の通知または表示を予約の要求元に対して行なうことを特徴とする(1)、(9)、(10)、(11)に記載の暗号処理装置、あるいは、方法とする。

**【0030】**

(14) アプリケーションの予約を受け付け、仮にスケジュール登録する予約登録手順と、受け付けたアプリケーションが、暗号アルゴリズムを使用するかどうかを判定し、暗号アルゴリズムを使用する場合は、それまでに受け付けている他のアプリケーションも含めて、各アプリケーションが使用する使用資源の量と、暗号アルゴリズムについては、複数用意されているそれぞれの暗号アルゴリズムについて使用資源の量とについて、暗号アルゴリズム毎に前記使用資源の合計値を算出する使用資源合計値算出手順と、スケジュールのどの時点でも、使用資源合計値が許容資源使用量を越えることのない暗号アルゴリズムであって、所定の条件に合致する暗号アルゴリズムを選択する暗号アルゴリズム選択手順と、受け付けたアプリケーションと選択した暗号アルゴリズムとをスケジュールに登録するスケジュール登録手順とを備えたことを特徴とする暗号処理方法とする。

**【0031】**

(15) 暗号通信アプリケーションの開始予定時刻以前の時間帯における(許容資源使用量－使用資源合計値)に基づき、暗号通信用の鍵を生成する前処理の



開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にする手順を有することを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 2 】

（１６）暗号アルゴリズムの使用開始予定時刻、あるいは、切替予定時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の鍵を生成する前処理の開始時刻を求め、暗号通信用の鍵を生成する前処理をスケジュールするようにし、前処理を含めた使用資源の合計値を許容資源使用量以下にする手順を有することを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 3 】

（１７）暗号通信用の鍵の寿命満了時刻以前の時間帯における（許容資源使用量－使用資源合計値）に基づき、暗号通信用の更新鍵を生成するリキー処理の開示時刻を求め、リキー処理をスケジュールするようにし、リキー処理を含めた使用資源の合計値を許容資源使用量以下にする手順を有することを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 4 】

（１８）前記使用資源の値について、その少なくともひとつは、予め設定された値、または、監視手順により計測された値であることを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 5 】

（１９）前記使用資源の値について、その少なくともひとつは、監視手順による計測に基づき初期設定された値、または、監視手順により計測更新された値であることを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 6 】

（２０）複数の暗号アルゴリズムを選択し、途中で切り替えて使用するようにしたことを特徴とする（１４）に記載の暗号処理方法とする。

#### 【 0 0 3 7 】

（２１）暗号アルゴリズムを途中で切り替え、再び元の暗号アルゴリズムを使用する場合、暗号通信用の鍵を生成する前処理における生成結果を記憶しておき

再利用するようにしたことを特徴とする（20）に記載の暗号処理方法とする。

#### 【0038】

（22）前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、予約済み暗号通信アプリケーションおよび予約要求暗号通信アプリケーションに対して、必要なら前記一定条件にかかわらず、暗号アルゴリズムの再選択のための計算を行い、登録可能なら、再選択を実施して予約登録を行うことを特徴とする（14）に記載の暗号処理方法とする。

#### 【0039】

（23）前記使用資源合計値が許容資源使用量を越える場合、または、所定条件に合致する暗号アルゴリズムがない場合、他のアプリケーションの実行時間を変更する、暗号通信平均データ転送量を低減するなどの変更、もしくはこれに限らない変更を行い、必要なら前記一定条件にかかわらず、再選択を実施して予約登録を行うことを可能にしたことを特徴とする（14）に記載の暗号処理方法とする。

#### 【0040】

（24）いずれかのアプリケーションの予約が取り消された場合、暗号通信アプリケーションの暗号アルゴリズムを再選択することを可能にしたことを特徴とする（14）に記載の暗号処理方法とする。

#### 【0041】

（25）前記変更、または、再選択を、予約要求元の指示に基づき行なうことを特徴とする（22）、（23）、（24）に記載の暗号処理方法とする。

#### 【0042】

（26）使用資源合計値が許容資源使用量を越える場合、または、暗号アルゴリズムが選択できない場合、予約ができない旨の通知または表示を予約の要求元に対して行なうことを特徴とする（14）、（22）、（23）、（24）に記載の暗号処理方法とする。

#### 【0043】

（27）（14）～（26）のいずれかに記載の方法を、コンピュータに機能

させるためのプログラムとして記録した記録媒体とする。

#### 【0044】

(28) (14) ~ (26) のいずれかに記載の方法を、コンピュータに機能させるためのプログラムとする。

#### 【0045】

##### 【発明の実施の形態】

以下、本発明の実施の形態を、図面を参照して説明する。

#### 【0046】

##### (実施の形態1)

図1は、本発明の(実施の形態1)に係わる暗号処理装置の構成を示すブロック図である。図1を参照すると、暗号処理装置は、スケジュール部10、アプリケーション11、12、暗号通信アプリケーション13、14、暗号情報決定部15、通信処理部16、暗号処理部17、リソース監視部18を備えている。以下、本暗号処理装置は、TV受信、TV録画、録画番組の再生、カメラ映像の暗号通信による受信と表示等の機能を有するものとして説明する。

#### 【0047】

スケジュール部10は、リモコンや外部からの予約指令に従って、各アプリケーションの予約の登録、実行時刻の管理と実行の制御を行なう。アプリケーション11は、一例として、テレビ放送を受信した映像データをハードディスクメモリに録画し、タイムシフトして再生するアプリケーションであり、アプリケーション名をAとする。テレビ放送の録画をタスクaとし、タイムシフト再生をタスクcとする。暗号通信アプリケーション13は、一例として、ネットワークカメラから送られるカメラ映像データを復号化し、テレビ画面に表示するアプリケーションであり、アプリケーション名をBとする。アプリケーションBは、タスクbより成り、暗号アルゴリズムを使用する。

#### 【0048】

暗号情報決定部15は、使用する暗号アルゴリズムのネゴシエーションにおける、暗号アルゴリズムの選択、提案、決定に必要な各種情報、例えば、各暗号アルゴリズムが消費する使用資源情報、暗号強度情報など、および、暗号通信に必

要な各種情報、例えば、暗号化・復号化に使用する公開鍵、秘密鍵、共有鍵などの鍵に関する情報などを管理し、使用する暗号アルゴリズムを選択、決定する。

#### 【0049】

暗号処理部17は、複数の暗号アルゴリズム処理手段、あるいは、処理手順を実行するプログラムを備えており、ネゴシエーションパケットの処理、暗号化・復号化に使用する鍵、公開値、公開鍵、秘密鍵、共有鍵などの作成、送信するデータの暗号化と受信したデータの復号化などを行なう。

#### 【0050】

通信処理部16は、暗号処理部17が作成したパケットをインターネット回線網に所定の通信プロトコルの形式にして送信し、インターネット回線網から受信した通信プロトコルの形式のデータからパケットを取り出して暗号処理部17に渡す。

#### 【0051】

次に、暗号処理装置の動作について説明する。

#### 【0052】

まず、TV録画を行う際の動作について説明する。図1の暗号処理装置において、受像機能部（図示しない）は、TV放送データを受信し、続いて、受信されたTV放送データを、録画機能部が内蔵する蓄積媒体（図示しない）に記録する。この処理は、アプリケーション11中のタスクaの処理を、本暗号処理装置内蔵のCPUに行なわせて実行する。録画したいチャンネルのTV番組の放送開始時刻から放送終了時刻まで、録画を連続的に行うことで、TV録画が完了する。

#### 【0053】

TV録画の予約は、予めリモコンから録画チャンネル番号、録画開始時刻、録画終了時刻の指示が出された際、その指示内容をスケジュール部10が受取り、後述するスケジュール・使用資源表100に登録する。

#### 【0054】

また、アプリケーション11は、録画したTV番組を、タイムシフトして再生する機能、タスクcを含んでいる。このタイムシフト再生のタスクcについても、リモコン予約により、再生番組番号、再生開始時刻、再生終了時刻が指示され

、その指示内容が、スケジュール部 10 により、スケジュール・使用資源表 100 に登録される。

#### 【0055】

次にネットワークカメラの映像をディスプレイに表示する際の、システムの動作について説明する。この処理は、暗号通信を行うための前処理と、実際にネットワークカメラアプリケーションを動作させる処理の 2 つに分かれる。暗号通信を行うための前処理については後述し、はじめに、実際にネットワークカメラアプリケーションを動作させる処理の概要について述べる。まず、ネットワークカメラでは、図 9 で説明したように、撮影機能部（図示しない）が撮影した映像データを、暗号通信アプリケーション 84 が、暗号処理部 87 に渡して、暗号処理部 87 が暗号化し、通信処理部 86 を介してインターネット回線網に送る。図 1 の暗号処理装置では、通信処理部 16 でインターネット回線網からパケットを受信し、暗号処理部 17 で復号化し、復号化された映像データを暗号通信アプリケーション 13 に渡し、暗号通信アプリケーション 13 は、映像データを所定の位置・大きさにディスプレイ（図示しない）に出力する。そして、ディスプレイが映像を表示する。以上のようにして、ネットワークカメラで撮影された映像がディスプレイに表示される。

#### 【0056】

ネットワークカメラの映像データを受信する時間帯の予約指示も、予めリモコンから、スケジュール部 10 に対して行なわれ、スケジュール・使用資源表 100 に登録される。

#### 【0057】

次に、スケジュール・使用資源表 100 について説明する。図 3 の（1）にその一例を示す。図 3 の（1）において、TV 録画のアプリケーション 11 である A は、タスク a とタスク c よりなる。TV 録画のタスク a は、2002 年 11 月 1 日の 12:00 から 13:00 までの番組を予約録画するように指令されているので、開始時刻欄と終了時刻欄に、その旨登録されている。図示しないが、この他のデータとして、チャンネル番号や番組コードなどが、登録される。タスク c は、録画した番組を 30 分遅れで、タイムシフトして見るアプリケーション A

の機能の一部であり、2002年11月1日の12:30から13:30まで実行するように予約され、登録されている。図示しないが、この他のデータとして、録画された番組のチャンネル番号や番組コード、あるいは、HDD内の番組ファイル管理コードなどが登録される。アプリケーションBは、暗号通信アプリケーション13において実行されるネットワークカメラの映像データの受信と表示機能であり、タスクbより成る。このタスクbは、2002年11月1日の11:45から以降継続して実行されるように、リモコンにより指示されており、スケジュール・使用資源表100の開始時刻と終了時刻に、その旨、登録されている。

#### 【0058】

また、スケジュール・使用資源表100には、各タスクa、b、c、それぞれの実行に必要とする使用資源の量、すなわち、CPUの処理能力、メモリ量、通信する場合のデータ転送量が、平均使用CPU資源（メガインストラクション／秒：MIPS）、平均使用メモリ資源（メガバイト：MB）、暗号通信の平均データ転送量（メガビット／秒：Mbps）として、記憶されている。タスクa、cは、暗号通信を行なわないので、暗号通信平均データ転送量は、0Mbpsである。暗号通信欄には、暗号通信の有無を記載してある。タスクbにおいて、暗号通信が「する」となっている。また、必要暗号強度の欄には、暗号通信の際の必要暗号強度を指定している。この例では、タスクbにおいて、暗号強度の1位、2位、3位のものの中から選ぶように指定されている。

#### 【0059】

暗号情報決定部15は、内部に暗号処理使用資源表150を備えている。暗号処理使用資源表150の例を、図3の（2）に示す。図3の（2）において、暗号処理部17が、保有している2種の暗号アルゴリズム、DES-CBC、3DES-CBCについて、それぞれの使用資源の量、すなわち、平均使用CPU資源（単位：MIPS／Mbps）、平均使用メモリ資源（MB）と、暗号順位とが記憶されている。平均使用CPU資源の単位は、この例においては、1Mbpsのデータ転送量を暗号化・復号化する際に必要なCPU処理能力をしめす。データ転送量が多いほど、暗号化・復号化の処理能力が比例的に多く必要になる。

1Mbps のデータを転送する場合は、それぞれ 100MIPS、300MIPS の CPU 処理能力を消費することを示している。

#### 【0060】

図5は、スケジュール・使用資源表100と暗号処理使用資源表150を基に、CPU使用率の時間推移を示した図である。CPU使用率は、CPUの最大処理能力を1000MIPSとした場合の、%で表示している。破線は、暗号アルゴリズムとして、DES-CBCを使用した場合、一点鎖線は、3DES-CBCを採用した場合である。タスクaとタスクcに加えてタスクbを処理する12:30～13:00の区間で、CPU使用率が最も高くなっている。CPU使用率は、処理量の瞬間的揺らぎや、予測できない緊急の処理に対応できるように、余裕を残すようにするのが一般的である。正常な処理を行なうのに支障がない許容総平均CPU使用率を50%とした場合、図5では、3DES-CBCの場合、12:00～13:00において、50%を超えるため、正常な処理に支障をきたす恐れがあることになる。DES-CBCなら、全時間において、50%以下である。

#### 【0061】

本発明では、スケジュール・使用資源表100と暗号処理使用資源表150を使用して、許容資源使用量、すなわち、許容総平均CPU使用率（または許容CPU処理能力）を超えないように、暗号アルゴリズムをスケジューリングする。

#### 【0062】

このために、次のようなスケジュール解析処理を行なう。スケジュール部10は、スケジュール・使用資源表100の内容と内部時計を監視する。内部時計の現在時刻より一定時間後、例えば、5分後のイベントの有無を調べる。図3（1）のスケジュール・使用資源表によれば、現在時刻11:40以前では、5分後のイベントがないので、スケジュール部10は、待機状態である。11:40になると、スケジュール部10は、5分後にイベントが予定されていることを検知する。検知すると、スケジュール部10は、スケジュール・使用資源表100内に登録された全タスクを調べ、それらの開始時刻、終了時刻によって区切られる各イベント区間ごとに、平均使用CPU資源の合計値を算出する。暗号通信を行

なうタスク b では、暗号強度第 3 位以上の暗号アルゴリズムから選択することが指定されているので、暗号処理使用資源表 150 に記載された各暗号アルゴリズムそれぞれを適用した場合の、平均使用 CPU 資源の合計値を算出する。

#### 【0063】

なお、5 分後のイベントの有無を調べる代わりに、アプリケーションが予約された時点において、上記平均使用 CPU 資源の合計値を算出するようにしてもよい。

#### 【0064】

図 4 は、合計値を算出するためにスケジュール部 10 が作成するイベント・使用資源表 110 の例である。図 4 (1) は、DES-CBC を使用した場合である。各イベント時刻毎に、タスク名毎の稼動と非稼動の別とその使用資源、暗号アルゴリズム名とその使用資源、および、使用資源合計の欄が設けられる。タスクが複数ある場合は、その数だけの欄が設けられる。各欄には、そのイベント時刻から次の行のイベント時刻までの間、実行すべきタスクや暗号アルゴリズムについての記入が行われる。すなわち、各イベント時刻から次のイベント時刻の間に予約されているタスク名とその使用資源量を記載する。タスクを終了する場合は、そのイベント時刻の行を設けるが、終了すべきタスク名を記載しないようにすればよい。暗号アルゴリズムを使用する場合は、暗号アルゴリズム名とその使用資源量も記載する。DES-CBC は、図 3 の例では 100 MIPS / Mbps であるが、カメラアプリケーションにおける映像データの暗号通信における平均データ転送量が、図 3 の例では 1 Mbps であるので、DES-CBC の平均使用 CPU 資源は、100 MIPS になる。図 4 (2) は、3DES-CBC を使用した場合のイベント・使用資源表 110 である。使用資源合計の欄を、CPU 処理能力 1000 MIPS に対して % 表示すれば、図 5 の破線と一点鎖線の CPU 使用率 (%) の時間推移になる。

#### 【0065】

スケジュール部 10 は、作成したイベント・使用資源表 110 の使用資源合計欄を調べ、最大 CPU 処理能力 1000 MIPS の許容総平均 CPU 使用率 50 % である許容 CPU 処理能力 500 MIPS を超えないすべての暗号アルゴリズム



ムを選択し、暗号アルゴリズム名を暗号情報決定部15に通知する。暗号情報決定部15は、通知された暗号アルゴリズム名と暗号処理使用資源表150とを参照して通知された暗号アルゴリズムの中から最も暗号強度が強いものを選択する。本実施の形態では、DES-CBCのみが通知されているので、この暗号アルゴリズムが選択される。

#### 【0066】

つぎに、暗号情報決定部15は、採用したDES-CBCを使用することをスケジュール部10に通知する。スケジュール部10は、通知された暗号アルゴリズムの使用をスケジュール化する。この例では、図4(1)を選択する。以上で、スケジュール解析に基く暗号アルゴリズムの選択とその使用スケジュールが作成できた。

#### 【0067】

スケジュール部10は、通知された暗号アルゴリズムDES-CBCに対応する図4(1)のイベント・使用資源表110を使用して、予約された各アプリケーションの起動、実行、停止を制御する。スケジュール部10は、常時イベント・使用資源表110(図4(1))を参照しており、内部時計が、11:45になると、スケジュール部10は、暗号通信アプリケーション13に対してタスクbを起動するよう指示し、暗号処理部17に対してDES-CBCを使用して暗号通信の前処理を行なうように指示する。

#### 【0068】

暗号処理部17は、暗号通信の前処理として、暗号通信に必要な共有鍵の作成のため、通信相手である図9のネットワークカメラの暗号処理部87との間で、ネゴシエーションを行ない、Diffie-Hellman、IKE、IPsecなどの仕様にしたがって、共有鍵を作成する。暗号処理部17、87の両方で共有鍵の作成が終了すると、暗号処理装置では、暗号処理部17が、暗号通信アプリケーション13に、暗号通信ができることを通知し、ネットワークカメラでは、暗号処理部87、暗号通信アプリケーション84に、暗号通信ができることを通知する。通知を受けた暗号通信アプリケーション84は、カメラの映像データを暗号処理部87に送り込み、暗号処理部87は、DES-CBCにより映像

データを暗号化し、通信処理部 86 は、暗号化された映像データパケットを作成してインターネット回線網を介して通信処理部 16 にパケットを送る。暗号処理部 17 は、通信処理部 16 より受信したデータを受取り、暗号の復号化を行ない、映像データを暗号通信アプリケーション 13 に渡す。暗号通信アプリケーション 13 は、既に説明したように、映像をディスプレイに表示する。スケジュール部 10 が、内部時計により 12:00 を検知すると、イベント・使用資源表 110 に従い、タスク b を継続し、タスク a、すなわち、アプリケーション 11 を起動する。12:30 になると、さらにタスク c を起動する。13:00 になると、タスク a がないので、タスク a を停止する。13:30 になると、タスク c がないので、タスク c を停止する。すなわち、各イベント時刻になると、その欄の内容をひとつ前のイベント時刻欄の内容と比較し、追加されたタスクや暗号アルゴリズムを起動し、記載がなくなったタスクや暗号アルゴリズムがあれば、それらを停止する。

#### 【0069】

以上のように、この（実施の形態 1）の暗号処理装置、あるいは、暗号処理方法では、スケジュール部 10 が、スケジュール・使用資源表 100 の予約内容と暗号処理使用資源表 150 のデータを調べることにより、使用 CPU 資源量が、許容 CPU 処理能力を超えないような暗号アルゴリズムを選択するスケジュールを作成するようにした。従って、暗号通信の実行中に、使用 CPU 資源量が、許容 CPU 処理能力を超えて、システムが破綻したり、暗号通信が中断するような危険性を予め排除できる。

#### 【0070】

各タスク a、b、c の使用資源の量である、平均使用 CPU 資源、平均使用メモリ資源、平均データ転送量などの数値は、予め暗号処理装置の製造や出荷時に、あるいは、各アプリケーションプログラムをインターネット回線網や、TV データ放送などの外部からのダウンロードする際に、各アプリケーション 11、13 の内部に記憶しておいてもよい。暗号アルゴリズムの平均使用 CPU 資源、平均使用メモリ資源、暗号順位、後述する前処理命令数、などは、暗号処理部 17 中の各暗号アルゴリズム実行手順の中にテーブルを設け、暗号・復号情報として

記憶しておいてもよい。この場合は、これらの暗号・復号情報を、暗号情報決定部15が読み出して、暗号処理使用資源表150に書きこむ。あるいは、暗号処理使用資源表150中に記憶しておいてもよい。

#### 【0071】

あるいは、平均使用CPU資源、平均使用メモリ資源、平均データ転送量、後述する前処理命令数、などを、前回実行時に計測しておき、計測したデータを所定のテーブルに記憶するようにしてもよい。この計測は、リソース監視部18において行ない、計測した情報をリソース監視部18に記憶しておく。予約を受けてスケジュール・使用資源表100を作成する際に、これらのデータを読み出して、スケジュール・使用資源表100の所定欄に書き込む。暗号アルゴリズムに関するデータは、計測結果を暗号処理使用資源表150に転送してもよい。一般に、CPU処理能力の使用量の計測は、モニタープログラムや、カーネルプログラムの一部として行なう。実行タスクのCPU処理能力の使用量を、CPU自身が計測できる場合は、リソース監視部18は、計測結果の記憶、管理を行なえばよい。

#### 【0072】

なお、図4（1）と図4（2）のイベント・使用資源表110は、後述する（実施の形態3）で説明する図6（1）、（2）のように、表の共通部分をまとめてひとつの表の形にしてもよい。

#### 【0073】

図2は、上記説明した処理を行なう暗号処理装置のハードウェア構成の例である。図2において、CPU25、ROM26、RAM27、HDD30、モデム36は、転送手段24であるバスラインに接続されており、標準的なコンピュータシステムの構成である。ROM26には、システム起動用のプログラムや書き換ええないデータが格納されている。HDD30内の、エリア31には、システム全体の統括や種々の制御を行なうオペレーションシステム（OS）のような制御プログラム、リソース監視部プログラム、通信処理部プログラムが格納されている。エリア32には、スケジュール部プログラム、暗号情報決定部プログラムが格納されている。エリア33には、暗号処理部プログラム、暗号アルゴリズムの

プログラムが格納されている。エリア 34 には、アプリケーションプログラム、暗号通信アプリケーションプログラムが格納されている。エリア 35 のファイル部には、テレビ録画番組が格納される。アンテナ 20 とチューナ 21 により受信されたテレビ番組の信号は、エリア 34 から RAM 27 に呼び出されたアプリケーションプログラム 11 に従って、CPU 25 と RAM 27 において、トランスポートストリームのデコードが行なわれ、エリア 35 のファイル部に録画される。また、録画されたデータは、タイムシフト時間の後に読み出され、CPU 25 と RAM 27 において、AV デコードの処理が行なわれ、デコードされた音声データと映像データは、音声処理 22 と表示処理 23 を介して、音声出力と映像出力として出力される。リモコン 29 の操作により指示される予約情報は、リモコン IF (インタフェース) 28 を介して、スケジュール部プログラムが受取り、スケジュール・使用資源表 100 に登録される。その後、スケジュール部プログラム、暗号情報決定部プログラム、暗号処理部プログラム、暗号アルゴリズムプログラム、アプリケーションプログラム、暗号通信プログラム、リソース監視部プログラム、通信処理部プログラムを、制御プログラムが CPU 25、RAM 27 を使用して、順次 RAM 27 上に呼び出し、CPU 25、RAM 27 が、各プログラムにしたがって、上記説明した処理を行なう。

#### 【0074】

次に、(実施の形態 1) を基本として、その他の実施の形態について説明してゆく。以下、各実施の形態の説明においては、ブロック構成が(実施の形態 1) の場合と同じ部分については繰り返しの説明を省き、異なる部分を中心に説明する。

#### 【0075】

##### (実施の形態 2)

図 1 で説明した(実施の形態 1) の暗号処理装置において、暗号通信に先立つ、前処理、すなわち、各種暗号通信にかかわるパラメータのネゴシエーションや共有鍵の交換の処理に無視できない時間がかかる場合には、予約した時間どおりに暗号通信を開始できない。(実施の形態 2) の暗号処理装置、あるいは、暗号処理方法は、このような課題を解決する。

## 【0076】

まず、図3(2)の暗号処理使用資源表150には、前処理命令数の欄を設け、各暗号アルゴリズム毎に、前処理に必要なCPU処理量を実行命令数 $I_m$ (単位MI：メガインストラクション)として記載しておく。この数値は、予め暗号処理装置の製造、あるいは、出荷時に記憶しておいてもよいし、前回に前処理を行なったときに、CPUの実行命令数を計測しておき、これを記憶するようにしてもよい。計測する場合は、リソース監視部18において行ない、計測結果を、資源情報として暗号処理使用資源表150に記憶する。(実施の形態1)のイベント・使用資源表110作成時に、暗号通信タスクbの開始イベント以前の時間帯における(許容CPU処理能力－使用資源合計)＝CPU処理能力余裕値 $Y_{cpu}$ (MIPS)を算出し、 $M_t(\text{秒}) = I_m / Y_{cpu}$ を求めると、前処理に必要な時間が求まる。

## 【0077】

なお、共有鍵の処理には、相手機器の処理時間と通信時間も必要である。相手機器の処理時間が無視できる場合は、上記計算値に余裕値 $\alpha$ を加算した値でもよい。無視できない場合は、相手機器の処理時間も考慮しなければならない。相手機器での処理時間が、本装置の処理時間とほぼ同等の場合は、 $M_t = (I_m / Y_{cpu}) \times 2 + \beta$ ( $\beta$ は通信時間および余裕時間)とすればよい。前回暗号通信時の処理時間を記憶しておいて、本装置と相手機器の処理時間の合計値に余裕時間を加算したものを $M_t$ とすればよい。本装置と同じように、相手機器も、そのCPU処理能力が状況により変動するなどの理由により、相手機器の処理時間が分からない場合は、相手機器に問い合わせる処理を行った後に $M_t$ を決定すればよい。いずれにしても、 $M_t = I_m / Y_{cpu} + \delta + \beta$ ( $\delta$ は相手機器の処理時間)とすればよい。

## 【0078】

イベント・使用資源表110のタスクbの開始イベント時刻を $M_t$ だけ早める。このようにすれば、暗号通信アプリケーション13のタスクbは、11:45の $M_t$ (秒)前に起動するから、前処理を完了する $M_t$ (秒)後、すなわち11:45に、暗号通信アプリケーション13の暗号通信が実際に行なえるようにな

る。このために、Mt だけ早いイベントを開始イベント時刻の前に追加挿入しておき、スケジュール部 10 が、11:45 の Mt (秒) 前に、前処理の開始を暗号処理部 17 に指示するようにし、前処理が完了した 11:45 に、タスク b を起動するようする。

#### 【0079】

本実施の形態によれば、暗号通信の前処理を行なうべき時間帯の CPU 処理能力余裕値 Ycpu が少ない場合には、より早めに前処理を開始でき、暗号通信を予約時間通りに開始することが可能になる。

#### 【0080】

(実施の形態 3)

つぎに、ひとつの暗号通信アプリケーションにおいて、許容 CPU 処理能力 Kcpu (MIPS) までの範囲で、暗号強度が最も大きい暗号アルゴリズムを切選択して使用するようにした実施の形態について説明する。本実施の形態の構成ブロック図は、図 1 の場合と同様である。前記 (実施の形態 1) と異なる部分について説明する。

#### 【0081】

図 5、または、図 4 を参照すると、許容 CPU 処理能力 Kcpu (MIPS) が 500 MIPS、すなわち、CPU 使用率が 50% の限界を超えない暗号アルゴリズムは、(11:45~12:00) と (13:00~以降) では、3DES-CBC と DES-CBC であるが、前者の方が暗号強度の順位が高い。スケジュール部 10 は、図 4 (1)、(2) のイベント・使用資源表 110 を各イベント区間ごとに、DES-CBC と 3DES-CBC とで比較し、使用資源合計が許容 CPU 処理能力 Kcpu (MIPS) = 500 MIPS を超えないものを、暗号情報決定部 15 に通知する。暗号情報決定部 15 は、通知された暗号アルゴリズム名が複数ある場合には、暗号強度が大きい方を選択し、スケジュール部 10 に通知する。スケジュール部 10 は、通知された暗号アルゴリズムの方の選択記入欄 (図示せず) に選択を示す選択コードを記入する。つぎに、(実施の形態 2) の場合と同様に、暗号アルゴリズムを切換えるイベント時刻の前の時間帯における (許容 CPU 処理能力 - 使用資源合計) = CPU 処理能力余裕値 Ycp

u (MIPS) を算出し、 $Mt \text{ (秒)} = Im / Ycpu$  を求める。切替イベント時刻の前  $Mt$  に、前処理のイベントを挿入する。このようなイベント・使用資源表 110 を作成した後、スケジュール部 10 は、イベント・使用資源表 110 (図 4 (1)、(2) の両方) を参照しながら、各アプリケーションや、次に使用する暗号アルゴリズムの前処理と暗号処理などの起動、実行、停止の制御を行なう。イベント・使用資源表 110 において、選択記入欄の選択コードを参照して、選択した方の暗号アルゴリズムの前処理と、暗号化・復号化の処理とを行なわせる。

#### 【0082】

図 6 (1) は、(実施の形態 3) で用いる、イベント・使用資源表 110 の別の一例である。イベント時刻欄には、年月日時刻の内、少なくとも時刻が記載される。タスク／資源欄には、予定タスク名と使用資源量 (MIPS) が記載される。使用資源量 (MIPS) は、平均使用 CPU 資源の量である。タスク／資源欄は、予約アプリケーションが増えると、必要に応じて、増設される。暗号／資源欄には、候補暗号アルゴリズム名と使用資源量 (MIPS) が記載される。資源合計欄には、予定タスクと候補暗号アルゴリズムによる使用資源合計 (MIPS) が記載される。暗号／資源欄と資源合計欄は、候補暗号アルゴリズムの数だけ設けられる。

#### 【0083】

使用暗号欄には、使用資源合計が許容 CPU 処理能力を超えない範囲で、暗号強度が最も高い暗号アルゴリズム名が記載される。この処理は、次のように行なえばよい。スケジュール部 10 が、各イベント区間毎に、使用資源合計が許容 CPU 処理能力を超えない候補暗号アルゴリズム名を暗号情報決定部 15 に通知する。暗号情報決定部 15 は、図 3 (2) の暗号処理使用資源表 150 を参照して、通知された候補暗号アルゴリズムから、暗号強度が最も高いものを選択し、その暗号アルゴリズム名をスケジュール部 10 に通知する。スケジュール部 10 は、通知された暗号アルゴリズム名を使用暗号欄に記載する。

#### 【0084】

このようなイベント・使用資源表を作成し、この表を基に、スケジュール部 1

0 が、各イベント区間に記載されたタスクと暗号アルゴリズムを起動、制御、停止することにより、予約されたアプリケーションを、CPU 処理能力の破綻なしに、実行することができる。

#### 【0085】

イベント・使用資源表は、図 6（1）の例に限らない。図 6（2）の暗号アルゴリズムの欄のように、暗号アルゴリズム名と資源の量とを別の欄に記載するようにしてもよい。

#### 【0086】

（実施の形態 4）

図 7 は、（実施の形態 3）において、暗号通信の前処理に無視できない時間がかかる場合に、（実施の形態 2）で説明したと同様に、前処理を早めに行なう場合のイベント・使用資源表の一例である。図 6（1）のイベント・使用資源表に、前処理欄と前処理暗号欄を追加する。前処理欄には、（実施の形態 3）において説明した、前処理にかかる時間  $M_t$ （秒） $= I_m / Y_{cpu}$  を記載する。前処理暗号欄には、前処理すべき暗号アルゴリズム名が記載される。なお、前処理欄はなくともよい。

#### 【0087】

つぎに、図 6（1）のイベント・使用資源表から、図 7 のイベント・使用資源表を作成する手順について説明する。最初に使用する予定の暗号アルゴリズム 3DES-CBC について、11:45 直前の状態における、 $M_t$ （秒） $= I_m / Y_{cpu}$  を計算する。この値が  $M_t = 180$ （秒）であったとする。11:45 より  $M_t$  だけ前に、前処理を開始する必要がある。11:45 の 180（秒） $= 3$  分前、すなわち、11:42 のイベント時刻欄を挿入する。前処理欄に、 $M_t 1 = 180$  を記載し、前処理暗号欄に 3DES-CBC の略号 3D を記載する。

#### 【0088】

12:00 には、DES-CBC に切り替えるので、この直前の状態における  $M_t$ （秒）を計算する。 $M_t = 120$ （秒）であったとする。12:00 までに前処理を完了する必要があるので、12:00 の 120（秒） $= 2$  分前、すなわち、11:58 のイベント時刻欄を挿入する。前処理欄に、 $M_t 2 = 120$  を記



載し、前処理暗号欄にDES-CBCの略号Dを記載する。

【0089】

13:00には、3DES-CBCに切り替えるので、この直前の状態におけるMt(秒)を計算する。Mt=225(秒)であったとする。13:00までに前処理を完了する必要があるので、13:00の225(秒)=3.75分=約4分前(15秒は余裕分である。)、すなわち、11:56のイベント時刻欄を挿入する。前処理欄に、Mt3=225を記載し、前処理暗号欄に3DES-CBCの略号3Dを記載する。

【0090】

挿入されたイベント欄の、タスク/資源、暗号/資源、資源合計の欄には、その上段の内容をコピーして記載する。

【0091】

このようにして作成したイベント・使用資源表を使用して、スケジュール部10は、前処理、各タスク、暗号アルゴリズムの起動、制御、停止を行なう。前処理を、暗号アルゴリズムの使用前に完了できるので、予約時間通りに、カメラアプリケーションを開始できる。

【0092】

この場合、暗号処理部17は、ひとつの暗号アルゴリズムの実行と別の暗号アルゴリズムの前処理とを、並行して実行できるようにしておく。

【0093】

前処理を行なうべき時間帯において、他のタスクの追加や停止が行われる場合は、CPU処理能力余裕値Ycpu(MIPS)が一定値ではなく変動するから、Mt(秒)=Im/Ycpuでは求めることができない。前処理を完了しておくべき時刻から時間の早い方向へ、CPU処理能力余裕値Ycpu(MIPS)の積分値を求めてゆき、積分値が前処理に必要なCPU処理の実行命令数Im(単位MI:メガインストラクション)になる時間長を、Mt(秒)として適用すればよい。このような場合は、挿入するイベント欄は、暗号アルゴリズム使用開始や切換の直前ではなく、いくつか上段のイベント欄の間に挿入することになる。

## 【0094】

上記図7のイベント・使用資源表では、12:56に次に使用する3DES-CBCのための前処理を行うようにしたが、12:00に3DES-CBCからDES-CBCに変更した後も3DES-CBCの公開鍵、秘密鍵などを破棄せず3DES-CBCを再度使用できる状態としておき、12:56から設定した前処理を行わないようにしてもよい。このようにすれば、前処理の再実行によるCPU資源の消費を削減できる。

## 【0095】

(実施の形態5)

図8は、候補暗号アルゴリズムとして、DES-CBC、3DES-CBC、AES (Advanced Encryption Standard) が用意されている場合の、イベント・使用資源表110と暗号処理使用資源表150の例である。AESは、平均使用CPU資源量が多くない割に、暗号強度が大きく、3つの暗号アルゴリズムの中では、暗号強度が1位である。イベント・使用資源表110では、3つの候補暗号アルゴリズムに対応して、それぞれ資源合計が計算される。11:45のイベント時刻を例にとると、許容CPU処理能力500 (MIPS) を超えない暗号アルゴリズムは、DES-CBC、3DES-CBC、AESである。スケジューラ部10は、この3つを候補として暗号情報決定部15に通知する。また、図3のスケジュール・使用資源表100の11:45開始のタスクbで使用する暗号アルゴリズムは、第3位以上とする条件がついている。この情報も、スケジューラ部10から暗号情報決定部15に通知される。暗号情報決定部15は、図8(2)の暗号処理使用資源表150を参照して、3つの中から、第3位以上のものを選び、さらにその中で暗号強度順位が最も高いAESを選択し、スケジューラ部10に通知する。スケジューラ部10は、使用暗号欄の11:45イベント時刻の欄に、AES名(略号A)を記入する。

## 【0096】

(実施の形態6)

Diffie-Hellman交換やIKEによる共有鍵の交換では、共有鍵の寿命を設定することができるようになっている。ひとつの鍵を長時間使用する

と、その間に、鍵を盗まれて解読される危険性が増える。このため、新たな鍵、すなわち、更新鍵を作成しておき、適切な時間後には更新鍵に切り替えてゆくようにする方式である。このような鍵の寿命を設ける方式では、鍵の寿命が満了になる前に、次に使用する更新鍵の生成を完了しておく必要がある。更新鍵の生成を行なうことをリキー処理と呼ぶ。最初の鍵の生成、リキー処理の両方とも、鍵の生成には、暗号化や復号化と同様に、大きなCPU処理能力を必要とする場合が多い。したがって、鍵寿命満了時刻よりも充分前の時刻に、リキー処理を開始することが望まれる。リキー処理を行なうべき時間帯に、大きなCPU処理能力を消費するアプリケーションがあると、許容CPU処理能力を超える。あるいは、更新鍵の準備が間に合わなくなる。

#### 【0097】

本（実施の形態6）においては、鍵を更新するまでの鍵寿命の値と予約スケジュールに基く使用資源合計値の推移を考慮しながら、適切なリキー開始時刻を、イベント・使用資源表110にイベントとして追加することにする。

#### 【0098】

まず、暗号処理使用資源表150に鍵寿命時間の欄を設け、各暗号アルゴリズム毎に、設定する予定の鍵寿命時間 $J_t$ を記載する。なお、一般的には、全体の危険度を一定とするためには、アルゴリズムの暗号強度が高いほど、鍵の寿命を長くすることができる。暗号アルゴリズム使用の開始時刻を $C_t$ とする。また最初の鍵の使用開始時刻を $K_{t1}$ とする。最初の鍵の使用開始時刻は、 $K_{t1} = C_t$ であり、鍵の寿命満了時刻は、 $(C_t + J_t)$ である。時刻 $(C_t + J_t)$ の前の時間帯でのCPU処理能力余裕値 $Y_{cpu}$  (MIPS) とし、リキー処理に必要なCPU命令数を $I_r$  (単位MI：メガインストラクション) とする。リキーに必要な時間は、 $R_t = I_r / Y_{cpu}$ である。時刻 $(C_t + J_t - R_t)$ までにリキー処理を開始すれば、鍵の寿命満了時刻 $(C_t + J_t)$ までに、更新鍵を準備できる。

#### 【0099】

CPU処理能力余裕値 $Y_{cpu}$  (MIPS) が、リキー処理予定の時間帯において一定値ではなく変動する場合は、（実施の形態4）における前処理の場合と

同様の考え方により、リキー処理を完了しておくべき時刻 ( $C_t + J_t$ ) から時間の早い方向へ、CPU処理能力余裕値  $Y_{cpu}$  (MIPS) の積分値を求めてゆき、積分値がリキー処理に必要なCPU処理の実行命令数  $I_r$  になる時間長を、 $R_t$  として適用すればよい。

#### 【0100】

つぎに、リキー開始時刻 ( $C_t + J_t - R_t$ ) を、追加イベントとして、イベント・使用資源表 110 に挿入し、リキー処理欄を追加して、リキー処理をスケジュールに記入するようにする。この操作は、暗号通信の前処理で説明したと同様の操作を、スケジュール部 10 と暗号情報決定部 15 の間で行なえばよい。

#### 【0101】

次の更新鍵の寿命に対しては、鍵の寿命満了時刻が、( $C_t + 2 * J_t$ ) となるので、この時刻に対するリキー開始時刻を求め、追加イベントを設ければよい。同様の操作を、暗号アルゴリズムの使用終了予定のイベント時刻まで行なう。

#### 【0102】

このようにすれば、予定されるCPU処理能力余裕値  $Y_{cpu}$  (MIPS) に応じたりキー処理の計画を予め立てられるので、許容CPU処理能力を超過して、システムが破綻することが無くなる。

#### 【0103】

なお、 $R_t$  は、若干の余裕を持たせるために、一定時間分  $\alpha$  だけ長めにするのが安全である。

#### 【0104】

鍵の寿命を管理する場合、一般的には、1) 時間で管理する、(例えば、寿命を、鍵の生成後  $X$  秒後、使用開始から  $Y$  秒後、などとする)、2) データ転送量で管理する、(例えば、寿命を、 $m$  パケット処理後、 $n$  バイト処理後、などとする)、などの手法があるが、本実施の形態は、1) 時間で管理する手法の場合のうち、使用開始から  $Y$  秒後とする場合に適用できる。鍵の生成完了後の時間を鍵の寿命とする場合には、つぎのような工夫をすればよい。鍵の生成時刻は、本装置と相手機器とでは、同じ時刻でない場合がある。すなわち、鍵の生成においては、一般的に、相手から公開値を受け取ってから自分の秘密鍵を生成するため、

一方の鍵の寿命満了時刻は、公開値を受け取ってから自分の秘密鍵を生成するための時間分だけ遅くなる。この時間関係は、鍵の生成を起動する側の機器と、鍵の生成手順により決まる。このように一方の鍵の生成が他方よりも遅れる場合、早く生成される側の鍵の生成時刻を起点として  $J_t$  を鍵の寿命とすれば、時間  $J_t$  の間は、両方の鍵が寿命時間内になり、一方の鍵の寿命が寿命満了になることはない。また、本装置と相手機器とが通信により、双方の鍵の生成が完了したことを知ることができる場合は、その時点を鍵の寿命起算の時点とすればよく、双方の鍵の寿命満了時刻は一致する。

#### 【0105】

なお、上記説明では、本装置側の処理時間だけを例にして説明したが、共有鍵の処理には、相手機器の処理時間と通信時間も必要である。前処理での相手機器における鍵の生成処理時間を記憶しておいて、これに本装置での上記  $R_t = I_r / Y_{cpu}$  に余裕時間を加算したものを、全体の  $R_t$  とすればよい。相手機器の処理時間が無視できる場合は、上記  $R_t = I_r / Y_{cpu}$  に余裕値  $\alpha$  を加算した値でもよい。相手機器での処理時間が、本装置の処理時間とほぼ同等の場合は、 $R_t = (I_r / Y_{cpu}) \times 2 + \beta$  ( $\beta$  は通信時間および余裕時間) とすればよい。本装置の場合と同様に、相手機器でも、他の一般的なアプリケーションにより、処理時間が変わる可能性がある場合は、相手機器に処理時間を問い合わせる処理を行った後に  $R_t$  を決定すればよい。いずれにしても、 $R_t = I_r / Y_{cpu} + \delta + \beta$  ( $\delta$  は相手機器での処理時間) とすればよい。

#### 【0106】

すでに説明したように、リキー処理においては、暗号アルゴリズム使用の開始時刻  $C_t$  を起点として、鍵の寿命満了時刻 ( $C_t + J_t * n$ ) までに、鍵の生成を完了しなければならない。更新鍵の生成を前の鍵の寿命満了までに確実にを行うための余裕を確保するために、リキー処理を少し早めに開始すると、その分、鍵が早めに生成される。この鍵の寿命が  $J_t$  であると、つぎの鍵の寿命満了時刻 ( $C_t + J_t * (n + 1)$ ) よりも早く寿命満了となるおそれがある。このようなことを避けるには、スケジュール上の鍵更新の時間間隔よりも、リキー処理において設定する鍵寿命を少し長めにすればよい。

**【0107】**

(実施の形態7)

つぎに、イベント・使用資源表110から予定されるCPU処理能力余裕値 $Y_{cpu}$  (MIPS) の推移に応じて、鍵の寿命値を適切に設定する実施の形態について説明する。

**【0108】**

スケジュール部10と暗号情報決定部15が、使用する暗号アルゴリズムを選択した段階で、スケジュール部10は、スケジュール・使用資源表100、または、暗号処理使用資源表150を参照して、あるいは、イベント・使用資源表110を参照して、暗号アルゴリズム使用開始時刻 $C_t$ の前の時間帯におけるCPU処理能力余裕値 $Y_{cpu}$  (MIPS) を調べる。リキーに必要な時間、 $R_t = I_r / Y_{cpu}$  を求め、 $(R_t + \alpha)$  を計算し、この値を鍵の寿命として暗号情報決定部15に通知する。なお、 $\alpha$  は余裕値である。よって、鍵の寿命満了時刻は、 $(C_t + R_t + \alpha)$  になる。つぎに、 $(C_t + R_t + \alpha)$  の前の時間帯におけるCPU処理能力余裕値を調べ、リキーに必要な時間を計算し、次の更新鍵の寿命とする。このような処理を繰り返し、各リキー処理の開始時刻をイベントに追加する。鍵の寿命完了と同時に、リキーを開始し、リキー完了時に、新たに生成した鍵を即座に使用開始することができる。

**【0109】**

このようにすれば、CPU処理能力余裕値 $Y_{cpu}$  (MIPS) を有効に使用して、早めにリキー処理が行なえるので、鍵の寿命も短くでき、暗号通信の安全性を高く保てる。

**【0110】**

また、CPU処理能力余裕値 $Y_{cpu}$  (MIPS) の一部分のみを使用するようになれば、リキー処理時間は長くなり、その分だけ鍵の寿命時間を長くする必要があるが、かわりに、CPU処理能力に余裕を残せる。

**【0111】**

本実施の形態によれば、上記のように柔軟な処理を計画的に組み立てることができる。

**【0112】**

本実施の形態は、鍵の寿命を時間で管理する手法の場合に適用するのが好ましい。

**【0113】**

(実施の形態8)

図7で説明した(実施の形態4)と図8で説明した(実施の形態5)では、共有鍵を交換する前処理を、暗号アルゴリズムを使用する直前、および、切り替える直前に行なった。ひとつの暗号通信アプリケーションにおいて複数の暗号アルゴリズムを切り替えて使用する場合、暗号通信アプリケーションを開始する前に、必要な共有鍵をまとめて生成するようにしてもよい。図7を例に取れば、前処理のMt1、Mt2、Mt3を11:45までに順番に実行するようなイベントを挿入する。

**【0114】**

このように、早めに鍵を生成する場合は、鍵の寿命は、1) 使用開始からJ秒後、2) 使用開始から、mパケット処理後、3) 使用開始から、nバイト処理後、などとするのがよい。鍵の生成から算定する場合は、生成以降実際に鍵を使用するまでの時間を加算した寿命時間を設定すればよい。

**【0115】**

(実施の形態9)

予めスケジュールで「a秒後に処理負荷が高くなる」と予測される場合に、予め高強度・高負荷の暗号アルゴリズムと、低強度・低負荷の暗号アルゴリズムの両方の鍵を用意しておき、スケジュールで全体負荷が高くなるとわかっている時点以降は、低強度・低負荷のアルゴリズムに切り替える方式を取るようにしてもよい。この場合、切り替えた後に、高強度・高負荷のアルゴリズムの鍵情報を明示的に削除し、メモリ資源の浪費の低減を図ることが可能である。

**【0116】**

なお、鍵の寿命は通信相手と取り決めるのが一般であり、削除する場合は、それを通知する必要があるので、そのための通信処理負荷が発生する。この負荷も、スケジュール・使用資源表100、イベント・使用資源表110に組み込んで

もよい。

#### 【0 1 1 7】

なお、予め高強度・高負荷の暗号アルゴリズムの鍵の寿命を、全体負荷が高くなる時点まで（あるいはその前後まで）としておき、削除の通知の手順を省略するようにしてもよい。

#### 【0 1 1 8】

（実施の形態 1 0）

上記各実施の形態では、使用資源として、CPU処理能力（MIPS）に着目し、許容資源使用量である許容CPU処理能力の範囲での有効利用と、破綻の防止を行なうようにした。暗号処理装置の資源としては、この他に、使用メモリサイズ（MB）、内部バスラインの時間占有率（%）などがある。使用メモリサイズが、システムのRAMサイズ、たとえば、521MBを超えると、HDDへの待避が頻繁に起こり、一部のアプリケーションが予約通りに実行できなかつたり、サービスが一時止まってしまうなどの不具合が発生する。内部バスラインの時間占有率（%）が、100%を超えても同様の事態が起きる。使用資源、すなわち、平均の使用メモリサイズや内部バスラインの平均時間占有率を、最大値に対して、たとえば、50%程度の許容資源使用量に押さえるようにすれば、不具合の発生は実質上回避できる。

#### 【0 1 1 9】

使用メモリサイズや内部バスラインの時間占有率（%）の合計値についても、上記したスケジュール・使用資源表やイベント・使用資源表を作成し、最大値を超えない暗号アルゴリズムを選択するようにすることができる。

#### 【0 1 2 0】

また、CPU処理能力、使用メモリサイズ、バスラインの時間使用率のひとつについてだけでなく、2つ、あるいは、3つの総合的使用率により、暗号アルゴリズムの選択を行なうようにしてもよい。総合的使用率は、一例として、個々の使用率に重みを掛けた加重平均値で表すことができる。

#### 【0 1 2 1】

（実施の形態 1 1）



上記各実施の形態では、リモコンや外部からアプリケーションの実行を予約する。外部からの予約は、携帯型の情報機器や携帯電話から、インターネット回線網を介して行なわれることが想定される。

#### 【0122】

図1や図2の構成において、スケジュール登録用の専用のアプリケーションを設けておき、そこでスケジュール情報を受け付け、予約要求をスケジュール部10に通知して、スケジュール・使用資源表100に記載する方法をとることができる。また、各アプリケーションが、上記の受け付けるスケジュール情報のうち、自アプリケーションに関係したもののみを一旦受付け、そして、スケジュール部10に登録を要求する方法もとれる。後者は、アプリケーション特有の形式で登録することができる。

#### 【0123】

暗号処理部17には、IPsec、SSL、TLSなどの暗号通信を実現するプロトコルをひとつ、あるいは、複数方式備え、また、IKEなどの鍵情報取得（IKEは共有鍵交換により鍵情報を取得する。IKEは、Diffie-Hellmanアルゴリズムにより鍵交換を実現する。）を行なうプロトコルによるプログラムをひとつ、あるいは、複数方式備えておき、DES-CBC、3DES-CBC、AESなどの暗号アルゴリズムを呼び出して、暗号通信を行なうようにする。

#### 【0124】

（実施の形態12）

図10は、上記各実施の形態で説明した本発明の暗号処理方法の基本的な手順をフローチャートで示した図である。（Sxx）は、手順のステップ番号である。

#### 【0125】

（S100）の予約登録手順において、アプリケーションの予約を受付け、スケジュール登録する。この登録は、基本的には、仮の登録である。（S101）の平均使用CPU資源合計値算出手順において、受け付けたアプリケーションが、暗号通信を行なうものかどうか判定し、暗号通信の場合は、それまでに受け付

けている他のアプリケーションも含めて、平均使用CPU資源の合計値を算出する。暗号アルゴリズムについては、複数用意されているそれぞれの暗号アルゴリズムについて平均使用CPU資源の量を加算する。スケジュールのどの時点でも許容CPU処理能力を超えることがない暗号アルゴリズムが存在する場合、その暗号アルゴリズムを一次選択する。(S102)の暗号アルゴリズム選択手順においては、一次選択された暗号アルゴリズムの中から、必要暗号強度の条件に合致する暗号アルゴリズムを選択する。(S103)のスケジュール登録手順において、選択した暗号アルゴリズムの処理をスケジュールに登録する。

#### 【0126】

スケジュールのどのイベント区間でも許容CPU処理能力を超えることがない暗号アルゴリズムを一次選択するのではなく、各イベント区間毎に許容CPU処理能力を超えることがない暗号アルゴリズムを一次選択し、(S102)において、一次選択された暗号アルゴリズムの中から、必要暗号強度の条件に合致する暗号アルゴリズムを各イベント区間ごとに選択するようにしてもよい。このようにすれば、CPU処理能力に余裕がある区間においては、暗号強度がより高い暗号アルゴリズムを選択できる可能性が高まる。

#### 【0127】

上記各ステップにおいて、平均使用CPU資源合計値が許容CPU処理能力を超える場合、および、(S102)において所定条件に合致する暗号アルゴリズムがない場合、アプリケーションの予約ができないので、その旨の回答や表示を、予約の要求元に対して行なう。

#### 【0128】

このとき、予約の要求元に対してスケジュール情報を掲示し、仮登録、あるいは、既に予約登録済の暗号通信アプリケーションの暗号アルゴリズムの変更を要求元が行なうことができるようにして実行を優先させたり、最も負荷の高いもの、あるいは最も暗号強度の高いものから暗号アルゴリズムの再選択（強度を低下させる）を行なった場合の平均使用CPU資源合計値を算出して、登録可能な場合は上記暗号アルゴリズムの再選択を行なって新規暗号通信アプリケーションの登録を行なったりすることも可能とする。このためには、図3において説明した

必要暗号強度の条件を必要ならば緩くして、暗号強度の低い暗号アルゴリズムを選択対象に追加するようにすればよい。その上で暗号アルゴリズムの再選択を行う。また、暗号アルゴリズムを選択できなかったイベント区間に対して、緩めた条件下において、暗号強度の高い暗号アルゴリズムを再選択させるようにしてもよい。また、該当イベント区間に対してのみ、緩めて追加した暗号アルゴリズムの中から条件を満たす、より強い暗号アルゴリズムを選択するようにしてもよい。このような変更を自動的に行えるようにしてもよいし、予約要求元の選択により、上記方法の選択、暗号アルゴリズム自体の選択などを行えるようにしてもよい。

#### 【0129】

なお、必要暗号強度の条件を緩くしない場合もある。すなわち、暗号通信アプリケーションの暗号通信を新規に予約する際に、既に他の暗号通信アプリケーションの暗号アルゴリズムが登録されており、しかも、一定条件として「必要暗号強度第3位以上」のような条件があり、その条件下で暗号強度が第1位のアルゴリズムが採用されている場合において、新規の暗号通信アプリケーションの暗号通信を登録するために必要なCPU処理資源が不足している場合は、上記既に登録されている暗号アルゴリズムを上記一定条件は緩和しない範囲で暗号強度を低下させ、すなわち、暗号強度を第2位また第3位に下げることにより、CPU処理資源を一部解放して、新規暗号通信アプリケーションの暗号通信が予約可能であれば、このような再選択により両方の暗号通信アプリケーションの予約、登録が可能になる。

#### 【0130】

また、暗号アルゴリズムの再選択とは別に、アプリケーションの種類によっては、一般のアプリケーションも含めて、その実行開始時刻をずらしたり、暗号通信平均データ転送量を暗号通信アプリケーションによって制御できる場合はその値を低くしたりすることによって、平均使用CPU資源合計値を低減し、新規要求アプリケーションの登録を可能とするようにしてもよい。また、これらの変更を、要求元が行なう場合は、予約登録者を認識して、予約登録者のみが可能であるようにするようによい。

**【0131】**

図11は、更に詳しいフローチャートである。(S200)において、アプリケーションの予約があった場合、その予約を受け付ける。(S201)において、スケジュール・使用資源表100に予約を登録する。これは、仮登録である。(S202)において、スケジュール・使用資源表100を元にイベント・使用資源表110に追加する。(S203)において、予約が暗号通信アプリケーションかどうか判定する。YESなら、登録されている各種アプリケーションに加えて、用意されている複数種の暗号アルゴリズムのそれぞれを使用した場合の平均使用CPU資源の合計値を、各イベント区間について算出する。(S205)において、許容CPU処理能力を超えない場合の暗号アルゴリズムを候補として一次選択する。選択される数は、複数、ひとつ、無しのいずれかである。(S206)において、候補暗号アルゴリズムが一つ以上あるかどうか判定し、YESなら、(S207)において、所定の条件を満たす暗号アルゴリズムを選択する。所定の条件とは、図3(1)の必要暗号強度である。条件を満たす暗号アルゴリズムがあれば、(S208)において、YESと判定される。(S209)において、共有鍵交換などの前処理の開始時刻の算出を、既に説明した手順により行なう。(S210)において、鍵の寿命満了に備えたりキー処理の開始時刻の算出を既に説明した手順により行なう。(S211)において、選択した暗号アルゴリズムの使用時刻、前処理の実行時刻、リキー処理の開始時刻をスケジュールに登録する、すなわち、イベント・使用資源表110に挿入、追記する。(S212)において、待機する。次の予約に対して待機してもよい。イベント時刻が到来すれば、そのイベントを実行してゆく。

**【0132】**

(S203)においてNOであれば、予約されたアプリケーションは、暗号通信を伴わない。(S213)において、平均使用CPU資源の合計値を各イベント区間に対して算出する。(S214)において、合計値が、許容CPU処理能力未満であれば、YESであり、(S201)、(S202)での登録は、有効となる。(S214)においてNOであれば、(S201)、(S202)で登録したアプリケーションを(S215)において、消去する。さらに、(S21

6)において、「予約が不可能である。」、「予約を失敗した。」旨の通知を、予約要求元に対して行なう。(S206)、(S208)においてNOの場合、使用可能な暗号アルゴリズムが見つからなかったので、同様に(S215)、(S216)の処理を行なう。

#### 【0133】

図12は、許容CPU処理能力を超えたため、予約できなかった場合に、既存のアプリケーションのアルゴリズムを変更することにより、CPU処理能力の余裕を生み出し、予約要求に応えるようにした暗号処理装置、および、処理方法の手順のフローチャートである。図11の(S206)、(S208)、(S214)において、アルゴリズムが選択できなかった場合、すなわち、NOの場合、(S301)において、最も負荷が高い暗号アルゴリズムを使用予定の暗号通信アプリケーションを検索する。(S302)において、その暗号アルゴリズムを負荷が低いものに変更した場合、変更した暗号アルゴリズム、予約要求暗号通信アプリケーション、および、そこで使用する暗号アルゴリズムについて使用資源合計を算出し、(S303)において、許容CPU処理能力未満かどうか判定する。YESなら、暗号アルゴリズムの変更を確定し、変更した暗号アルゴリズム、予約要求暗号通信アプリケーション、および、そこで使用する暗号アルゴリズムについて、(S209)以降で、前処理、リキー処理なども含めたスケジュール確定を行う。(S303)において、許容CPU処理能力がまだ不足であれば、NOであるので、(S305)において、変更の余地のあるアプリケーションがまだあるかどうか調べ、YESなら(S301)に戻り、暗号アルゴリズム変更を試みる。(S305)においてNOなら、予約要求に対応することがまったく不可能であるので、(S215)に戻る。

#### 【0134】

図13は、予約要求元に、予約の変更を促すように表示を行い、予約要求元の判断により、暗号アルゴリズムの再選択を行う暗号処理装置、および、暗号処理方法の手順を示すフローチャートである。図11の(S206)、(S208)、(S214)において、アルゴリズムが選択できなかった場合、すなわち、NOの場合、(S400)において、予約要求元に再選択を促す表示を行う。予約

要求元は表示を見て、（S 4 0 1）において、最も負荷が高い暗号アルゴリズムを使用予定の暗号通信アプリケーションを検索し、選択する。暗号処理装置は、その手順に従い、（S 4 0 2）において、その暗号アルゴリズムを負荷が低いものに変更した場合、変更した暗号アルゴリズム、予約要求暗号通信アプリケーション、および、そこで使用する暗号アルゴリズムについて使用資源合計を算出し、（S 4 0 3）において、許容CPU処理能力未満かどうか判定する。YESなら、暗号アルゴリズムの変更を確定し、変更した暗号アルゴリズム、予約要求暗号通信アプリケーション、および、そこで使用する暗号アルゴリズムについて、（S 2 0 9）以降で、前処理、リキー処理なども含めたスケジュール確定を行う。（S 4 0 3）において、許容CPU処理能力がまだ不足であれば、NOであるので、（S 4 0 5）において、変更の余地のあるアプリケーションがまだあるかどうか調べ、YESなら（S 4 0 0）において、予約要求元に再選択を促す表示を行い、（S 4 0 1）以降、暗号アルゴリズム変更を試みる。（S 4 0 5）においてNOなら、予約要求に対応することがまったく不可能であるので、（S 2 1 5）に戻る。

#### 【0 1 3 5】

なお、上記のような再選択では、上記一定の条件を緩める場合もあるが、必要暗号強度の条件を緩くしない場合もある。すなわち、暗号通信アプリケーションの暗号通信を新規に予約する際に、既に他の暗号通信アプリケーションの暗号アルゴリズムが登録されており、しかも、一定条件として「必要暗号強度第3位以上」のような条件があり、その条件下で暗号強度が第1位のアルゴリズムが採用されている場合において、新規の暗号通信アプリケーションの暗号通信を登録するために必要なCPU処理資源が不足している場合は、上記既に登録されている暗号アルゴリズムを上記一定条件は緩和しない範囲で暗号強度を低下させ、すなわち、暗号強度を第2位また第3位に下げることにより、CPU処理資源を一部解放して、新規暗号通信アプリケーションの暗号通信が予約可能であれば、このような再選択により両方の暗号通信アプリケーションの予約、登録が可能になる。

#### 【0 1 3 6】

図 13 のフローチャートにおいて、(S401) では、ユーザである予約要求元に、暗号アルゴリズムを低い負荷のものに変更する暗号通信アプリケーションを指定させ、(S402) において、指定された暗号アルゴリズムを低い負荷のものに変更した場合の使用資源合計を算出するようにしてもよい。この方法は、予約済の暗号通信アプリケーションが複数ある場合に、特に有効である。あるいは、(S403) と (S404) の間に、変更可能な暗号通信アプリケーションがどれであるかを予約要求元が識別、あるいは選択できる情報と、現在予約登録されている暗号アルゴリズムと、選択、変更可能な、すなわち候補となる暗号アルゴリズムを提示し、予約要求元に実際に実施するか否かを判定させ、変更する内容を決めさせるようにしてもよい。予約要求元に対して、さらに、どのような暗号アルゴリズムを適用可能か、あるいは、それらの暗号アルゴリズムの暗号強度やその順位などの情報を表示、提供してもよい。予約要求元は、再選択するか否かの判断だけではなく、その内容までも考慮したうえでの判断を行うことができるようになる。

#### 【0137】

##### (実施の形態 13)

これまでに、暗号通信アプリケーション、前処理、リキー処理などを予約登録や追加登録する場合について説明した。スケジュール部 10 が、イベントを実行している最中に、新たな追加の予約登録の要求が発生した場合でも、上記各実施の形態において説明した許容資源量の余裕の範囲であれば、スケジュールの追加が可能である。スケジュール部 10 は、追加予約登録要求に対して、スケジュール・使用資源表 100 に仮登録し、作成済みのイベント・使用資源表 110 に、追加アプリケーションに関するタスク欄とその開始希望時刻イベント欄、終了希望時刻イベント欄を挿入したイベント・使用資源表を別途作成する。挿入した開始希望時刻イベント行と、終了希望時刻イベント行に上段の各タスクと暗号アルゴリズムの記載内容をコピーする。開始希望時刻イベント以降、終了希望イベントの前のイベントまでに追加使用希望の使用資源量を追記する。スケジュール部 10 と暗号情報決定部 15 は、使用資源量の合計の算定や、許容資源量との比較を行ない、許容資源量未満であれば、更に、必要に応じて暗号アルゴリズムの選

択などの作業を行ない、予約追加可能である場合には、この別途作成したイベント・使用資源表に切り替えることにより、追加予約希望のアプリケーションをイベント・使用資源表に追加することが可能になる。このような予約追加の判断にかかわる処理は、処理量が多くない。よって、使用資源は少なく、システムが破綻する可能性は実質上無く、処理時間も極めて短時間であるので、殆ど即座に対応することが可能である。なお、暗号アルゴリズムを使用する場合は、前処理の所要時間以上早めに予約要求を行なわなければ、その分、暗号通信の開始が少し遅れる。

#### 【0138】

反対に、あるアプリケーションの予約を取り消す場合は、該当するイベント時刻における、そのアプリケーションを構成するタスク名と、暗号通信の場合は更に、関連する暗号アルゴリズム名と使用資源を、記載欄から削除すればよい。この処理も、極めて短時間に行なえるが、スケジュール部10が、イベント・使用資源表110を参照して作業しているイベント時刻の前後を避けて行なうようにする方がよい。暗号アルゴリズムを使用するアプリケーションの場合は、関連する前処理やリキー処理のイベントについても、一緒に削除する。このとき、既に予約登録済みの他のアプリケーションのアルゴリズムを、予約元に掲示することによって変更を可能としたり、最も負荷の低いもの、あるいは最も暗号強度の低いものからアルゴリズムの再選択（強度を向上させる）を行なった場合の平均使用CPU資源合計値を算出して許容CPU処理能力を超えない場合はアルゴリズムの変更を実施したりすることも可能とする。また、アルゴリズムの再選択とは別に、アプリケーションの種類によっては、許容CPU処理能力を超えない範囲で実行開始時刻をずらしたり、暗号通信平均データ転送量をアプリケーションによって制御できる場合はその値を高くしたりすることによって、実行完了時刻を早めることも可能とする。また、これらの変更を、要求元が行なう場合は、予約登録者を認識して、予約登録者のみを変更できるようにする方法も提供してもよい。

#### 【0139】

図14は、いずれかのアプリケーションの予約を取り消した場合に、生まれた



許容CPU処理能力を暗号アルゴリズムの暗号強度の強化に振り向ける場合の、暗号処理装置、および、処理方法の手順のフローチャートである。予約取り消しを検知した場合、(S501)において、最も負荷が低い暗号アルゴリズムを使用する予定の暗号通信アプリケーションを検索する。(S502)において、その暗号アルゴリズムを暗号強度の高いものに変更した場合の使用資源合計を算出し、(S503)において、許容CPU処理能力未滿かどうか判定する。NOなら、許容CPU処理能力が不足であるので、暗号強度の強化はできず、(S212)に進む。YESなら、(S504)において、図11の(S209)、(S210)、(S211)と同様に、暗号アルゴリズムの変更に対応して、前処理、リキー処理なども含めたスケジュール確定を行う。(S505)において、変更の余地のあるアプリケーションがまだあるかどうか調べ、YESなら(S501)に戻り、暗号アルゴリズムの暗号強化を試みる。(S505)においてNOなら、(S212)に進む。

#### 【0140】

(実施の形態の変形、および、補足)

前記使用資源合計値が許容資源使用量を越える場合、および、所定条件に合致する暗号アルゴリズムがない場合について補足すると、予約済み暗号通信アプリケーションおよび予約要求暗号通信アプリケーションに対して、必要なら前記一定条件にかかわらず、暗号アルゴリズムの再選択のための計算を行い、登録可能なら、再選択を実施して予約登録を行うようにすることを行ってもよい。これは、予約済みの暗号通信アプリケーション用の暗号アルゴリズムが、前記一定条件を満たす暗号強度の中で強度が上位のものを採用している場合、一定条件はそのままでも、その条件下で、より暗号強度が低位のものに変更する操作を含む。また、このような変更の余地がない場合は、前記一定条件を緩和することを含む。また、前記使用資源合計値が許容資源使用量を越える場合、および、所定条件に合致する暗号アルゴリズムがない場合、他のアプリケーションの実行時間の変更、暗号通信平均データ転送量を低減する変更、もしくはこれに限らない変更を行い、必要なら前記一定条件にかかわらず、この条件を緩めるなどにより、再選択を実施して予約登録を行うことを可能にしてもよい。また、上記これに限らない

変更としては、他のアプリケーションの性能を低くしてCPU処理能力の消費量を減らすことができる場合は、このような変更を選択して、暗号アルゴリズムの処理にCPU処理能力を振り向けるようにしてもよい。

#### 【0 1 4 1】

上記説明において、許容CPU処理能力を50%とした。また、平均使用CPU資源を用いた。CPUは、アプリケーションの処理以外に、OSの処理やカーネルの処理などの基本的処理も並行して行なっている。また、アプリケーションの処理において、常に一定のCPU資源を使用するとは限らない。通信においてパケットが集中して到着する場合や、テレビ放送の送信においてデータレートが絵柄によって変動する場合などもあり、これらの変動を吸収する余裕が必要である。このために、平均使用CPU資源を用い、許容CPU処理能力を100%より小さい値としている。

#### 【0 1 4 2】

スケジュール・使用資源表100、イベント・使用資源表110、暗号処理使用資源表150の形式、表内の各数値は、上記例に限定されない。異なった形式でも、必要な情報が表現でき、資源の計算ができるものであれば、本発明に使用できる。イベント時刻は、分より細かい秒、あるいは秒以下の分解能を持たせてもよい。

#### 【0 1 4 3】

図1の構成では、暗号情報決定部15と暗号処理部17の間で暗号・復号情報を授受するようにしたが、暗号情報決定部15が、暗号通信アプリケーション13、14との間で、その暗号アプリケーションに対応した暗号・復号情報を授受し、暗号通信アプリケーション13、14が、暗号アプリケーション自身に対応した暗号・復号情報を、暗号処理部17との間で授受するようにしてもよい。

#### 【0 1 4 4】

図1の構成において、スケジュール部10と暗号情報決定部15とがひとつのブロックで成り、スケジュール・使用資源表100、暗号処理使用資源表150、および、イベント・使用資源表110の3つのテーブルを取り扱うようにしてもよい。

## 【0145】

また、図1の構成において、暗号情報決定部15と暗号処理部17がひとつのブロックで成り、暗号処理使用資源表150や暗号・復号情報を扱い、スケジュール部10、暗号通信アプリケーション13、14との間で、関係する情報をやり取りするようにしてもよい。

## 【0146】

本発明の暗号処理装置が相手の装置と暗号通信を行なう場合、両者が共に使用可能な暗号アルゴリズムを選択対象とするのが好ましい。本暗号処理装置が選択した暗号アルゴリズムが、相手装置で対応できない場合は、暗号通信ができなくなるのは言うまでもない。したがって、上記予約の段階で、相手装置との間で、使用可能な暗号アルゴリズムを共有化するネゴシエーションを行なうことが好ましい。

## 【0147】

通信におけるパケット送信時の揺らぎや、受信におけるパケットの順序の乱れや受信の遅れがあると、使用中の鍵から次の更新鍵に更新される時刻は、鍵の満了時刻の前後に揺らぐ可能性がある。特に受信側でその可能性が大きい。揺らぎ時間が累積してゆき、更新した鍵の使用開始時刻が、スケジュール時に予想した時刻よりも大幅にずれることが懸念される場合は、その分リキー処理開始時刻をずらしてもよい。送信側のネットワークカメラが、鍵の更新を、寿命満了時間に基づき行なう限りは、揺らぎ時間の累積は起こらない。

## 【0148】

上記暗号アルゴリズムが、認証アルゴリズム、あるいは圧縮アルゴリズムであっても、本発明が適用できる。よって、上記の各暗号アルゴリズムは、認証アルゴリズム、および圧縮アルゴリズムを含むものとする。

## 【0149】

なお、本発明の暗号処理方法のプログラムを記録した記録媒体は、プログラムを記録したROM、RAM、フレキシブルディスク、CD-ROM、DVD、メモリカード、ハードディスクなどの記録媒体をいう。また、電話回線、搬送路などの通信媒体も含む概念である。

## 【0150】

## 【発明の効果】

本発明の暗号処理装置、および、暗号処理方法によれば、1) 将来の動作を考慮して暗号アルゴリズムの選択など、暗号設定情報を決定することができるため、途中で暗号アルゴリズムを切り替えなくとも、処理資源が枯渇することを防止できる。2) 将来の動作を考慮して前もって共有鍵などの暗号・復号情報を用意できるため、必要なときにすぐに暗号通信を行なうことができる。また、資源の使用レベルが低いときに、共有鍵などの暗号・復号情報を用意しておける。3) 刻々かわる資源の使用状態に応じて暗号アルゴリズムの選択などを制御する動的な資源使用制御にくらべて、手後れになる危険性を低減できる。

## 【図面の簡単な説明】

## 【図1】

本発明の暗号処理装置、および、暗号処理方法の機能的構成を示すブロック図

## 【図2】

本発明の暗号処理装置、および、暗号処理方法を実行するシステムのブロック図

## 【図3】

本発明に使用するスケジュール・使用資源表と暗号処理使用資源表の例を示す図

## 【図4】

本発明に使用するイベント・使用資源表の例を示す図

## 【図5】

本発明に使用する資源の使用を表す図

## 【図6】

本発明に使用するイベント・使用資源表の例を示す図

## 【図7】

本発明に使用するイベント・使用資源表と暗号処理使用資源表の例を示す図

## 【図8】

本発明に使用するイベント・使用資源表と暗号処理使用資源表の例を示す図

**【図 9】**

従来の暗号処理方法の機能ブロック図

**【図 1 0】**

本発明の暗号処理方法の手順を示すフローチャート

**【図 1 1】**

本発明の暗号処理方法の手順を示すフローチャート

**【図 1 2】**

本発明の暗号処理方法の手順を示すフローチャート

**【図 1 3】**

本発明の暗号処理方法の手順を示すフローチャート

**【図 1 4】**

本発明の暗号処理方法の手順を示すフローチャート

**【符号の説明】**

1 0 スケジュール部

1 1, 1 2 アプリケーション

1 3, 1 4 暗号通信アプリケーション

1 5 暗号情報決定部

1 6 通信処理部

1 7 暗号処理部

1 8 リソース監視部

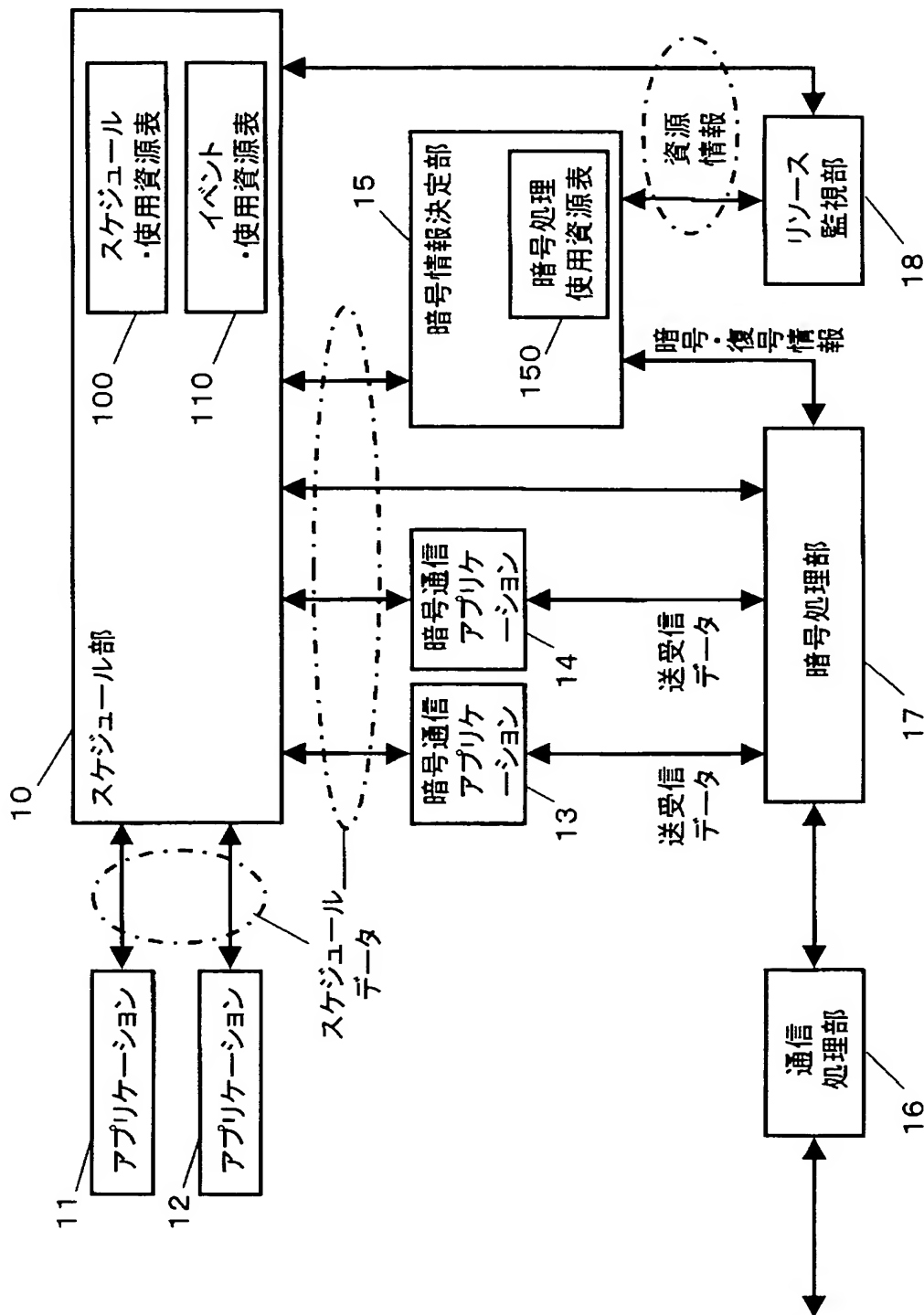
1 0 0 スケジュール・使用資源表

1 1 0 イベント・使用資源表

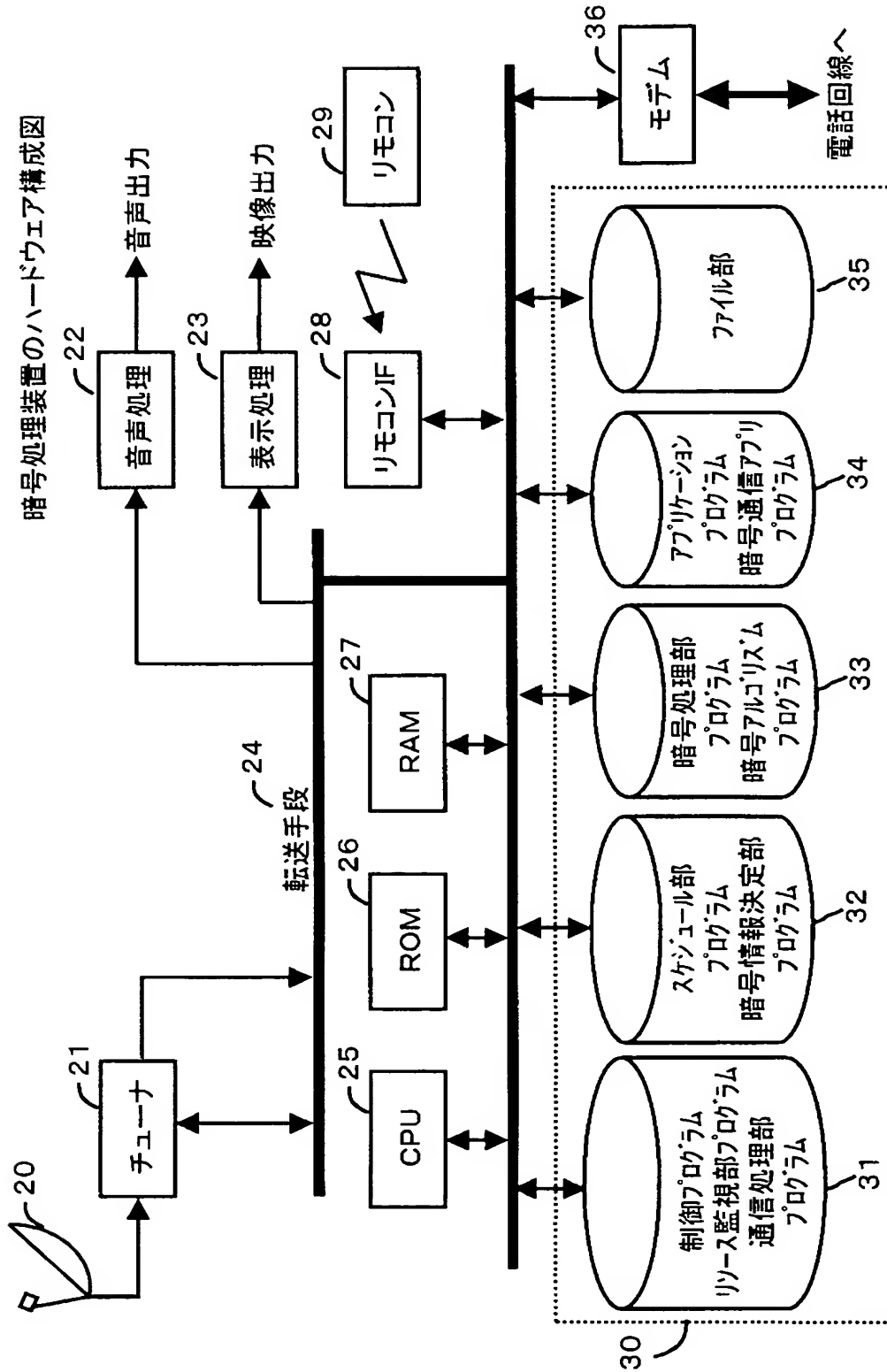
1 5 0 暗号処理使用資源表

【書類名】 図面

【図 1】



【図 2】



【図 3】

(1)スケジュール部のスケジュール・使用資源表

タスク	所属 アプリケーション	開始時刻	終了時刻	平均使用 CPU資源	平均使用 メモリ資源	平均データ 転送量	暗号通信	必要 暗号強度
タスクa	A	2002/11/1 12:00	2002/11/1 13:00	200MIPS	50MB	0Mbps	しない	—
タスクb	B	2002/11/1 11:45	— (未定)	50MIPS	20MB	1Mbps	する	第3位以上
タスクc	A	2002/11/1 12:30	2002/11/1 13:30	100MIPS	20MB	0Mbps	しない	—

(注：平均データ転送量は、暗号通信の平均データ転送量である。)

(2)暗号情報決定部の暗号処理使用資源表

暗号アルゴリズム	平均使用CPU資源 (MIPS/Mbps)	平均使用メモリ資源 (MB)	暗号強度 順位
DES-CBC	100	13	2
3DES-CBC	300	20	1



【図 4】

(1) スケジュール部のイベント・使用資源表 (DES-CBC)

イベント時刻	タスクb		タスクa		タスクc		暗号アルゴリズム		使用資源 合計
	動作状況	使用資源	動作状況	使用資源	動作状況	使用資源	アルゴリズム名	使用資源	
2002/11/1 11:45	稼動	50MIPS	非稼動		非稼動		DES-CBC	100MIPS	150MIPS
2002/11/1 12:00	稼動	50MIPS	稼動	200MIPS	非稼動		DES-CBC	100MIPS	350MIPS
2002/11/1 12:30	稼動	50MIPS	稼動	200MIPS	稼動	100MIPS	DES-CBC	100MIPS	450MIPS
2002/11/1 13:00	稼動	50MIPS	非稼動		稼動	100MIPS	DES-CBC	100MIPS	250MIPS
2002/11/1 13:30	稼動	50MIPS	非稼動		非稼動		DES-CBC	100MIPS	150MIPS

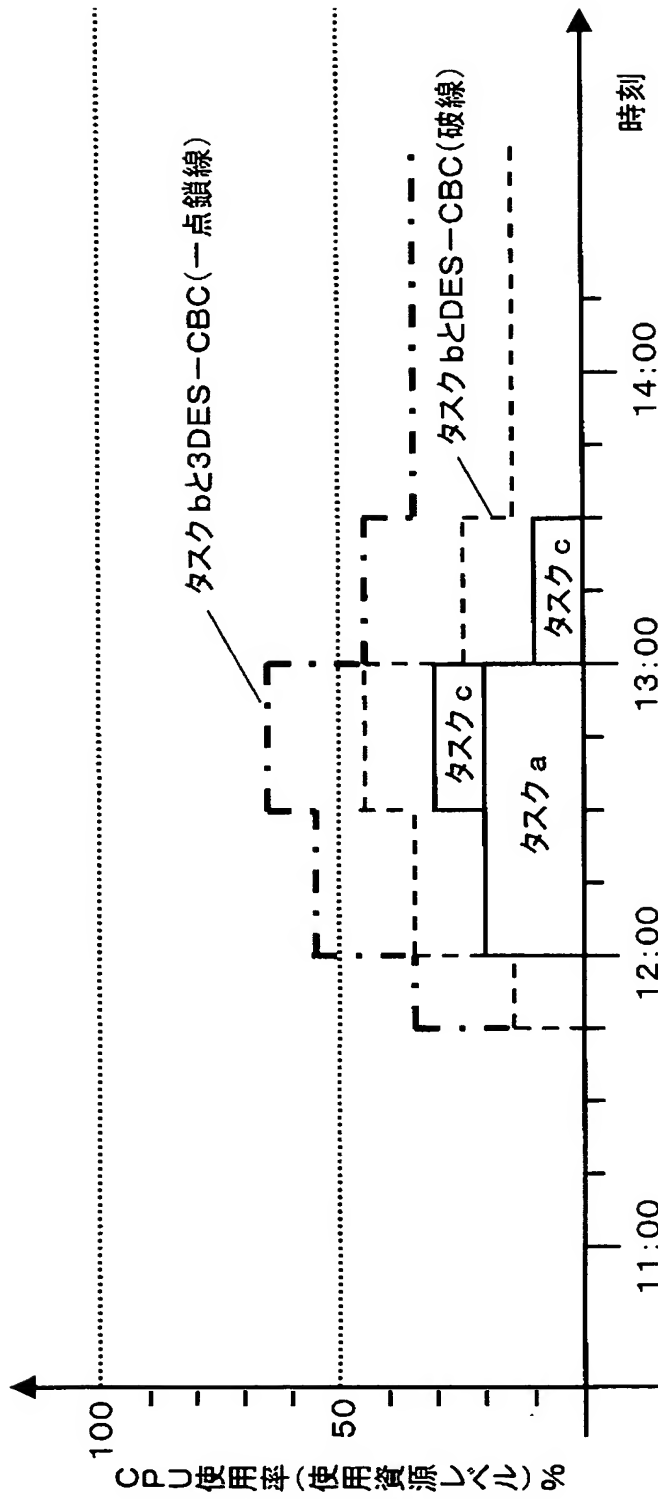
(使用資源は、平均使用CPU資源)

(2) スケジュール部のイベント・使用資源表 (3DES-CBC)

イベント時刻	タスクb		タスクa		タスクc		暗号アルゴリズム		使用資源 合計
	動作状況	使用資源	動作状況	使用資源	動作状況	使用資源	アルゴリズム名	使用資源	
2002/11/1 11:45	稼動	50MIPS	非稼動		非稼動		3DES-CBC	300MIPS	350MIPS
2002/11/1 12:00	稼動	50MIPS	稼動	200MIPS	非稼動		3DES-CBC	300MIPS	550MIPS
2002/11/1 12:30	稼動	50MIPS	稼動	200MIPS	稼動	100MIPS	3DES-CBC	300MIPS	650MIPS
2002/11/1 13:00	稼動	50MIPS	非稼動		稼動	100MIPS	3DES-CBC	300MIPS	450MIPS
2002/11/1 13:30	稼動	50MIPS	非稼動		非稼動		3DES-CBC	300MIPS	350MIPS

(使用資源は、平均使用CPU資源)

【図 5】



【図 6】

(1) スケジュール部のイベント・使用資源表 (DES-CBC、3DES-CBC)

イベント時刻	タスク/資源	タスク/資源	タスク/資源	暗号/資源	資源合計	暗号/資源	資源合計	使用暗号
11:45	b 50			D 100	150	3D 300	350	3D
12:00	b 50	a 200		D 100	350	3D 300	550	D
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D
13:00	b 50	c 100		D 100	250	3D 300	450	3D
13:30	b 50			D 100	150	3D 300	350	3D

(資源は平均使用CPU資源 (MIPS)、DはDES-CBC、3Dは3DES-CBC)

(2) スケジュール部のイベント・使用資源表 (DES-CBC、3DES-CBC) の別の例

イベント時刻	タスク/資源	タスク/資源	タスク/資源	タスクcで		タスクcで		使用暗号
				暗号 D の場合	暗号 3D の場合	暗号 D の場合	暗号 3D の場合	
				資源	資源合計	資源	資源合計	
11:45	b 50			100	150	300	350	3D
12:00	b 50	a 200		100	350	300	550	D
12:30	b 50	a 200	c 100	100	450	300	650	D
13:00	b 50	c 100		100	250	300	450	3D
13:30	b 50			100	150	300	350	3D

(資源は平均使用CPU資源 (MIPS)、DはDES-CBC、3Dは3DES-CBC)

【図 7】

(1)スケジュール部のイベント・使用資源表(DES-CBC、3DES-CBC)

イベント時刻	タスク/資源	タスク/資源	タスク/資源	暗号/資源	資源合計	暗号/資源	資源合計	使用暗号	前処理暗号
11:42									Mt1 3D
11:45	b 50			D 100	150	3D 300	350	3D	
11:58	同上			同上	同上	同上	同上	3D	D
12:00	b 50	a 200		D 100	350	3D 300	550	D	
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D	
12:56	同上	同上	同上	同上	同上	同上	同上	D	Mt3 3D
13:00	b 50	c 100		D 100	250	3D 300	450	3D	
13:30	b 50			D 100	150	3D 300	350	3D	

(資源は平均使用CPU資源(MIPS)、DはDES-CBC、3Dは3DES-CBC)

(2)暗号情報決定部の暗号処理使用資源表

暗号アルゴリズム	平均使用CPU資源(MIPS/Mbps)	前処理命令数(MI)	暗号強度順位
DES-CBC	100	100	2
3DES-CBC	300	300	1

【図 8】

(1)スケジュール部のイベント・使用資源表(DES-CBC、3DES-CBC、AES)

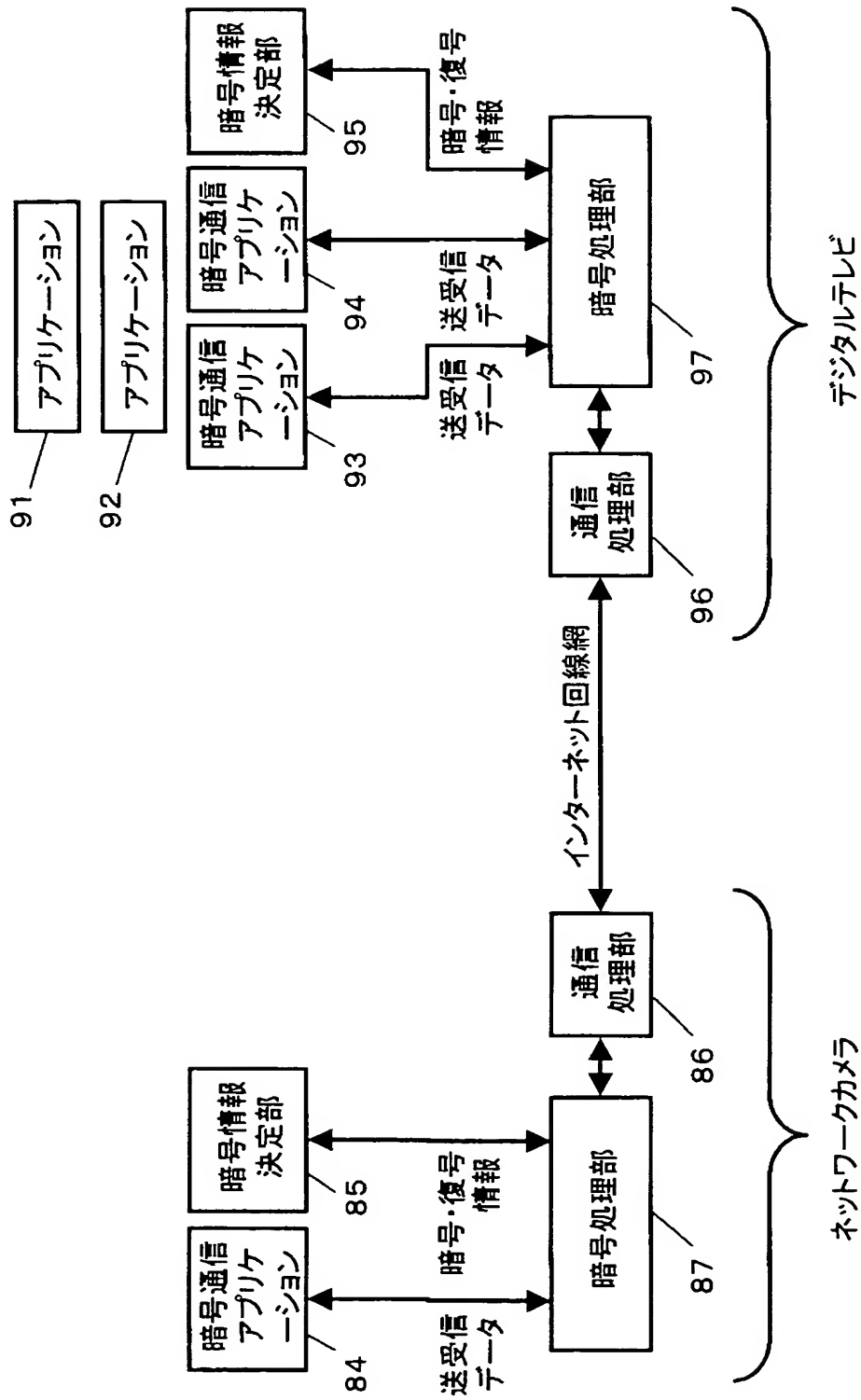
イベント時刻	タスク/資源	タスク/資源	タスク/資源	暗号/資源	資源合計	暗号/資源	資源合計	使用暗号	前処理	前処理暗号
11:43									Mt1	A
11:45	b 50			D 100	150	3D 300	350	A		
12:00	b 50	a 200		D 100	350	3D 300	550	A		
12:29	同上	同上		同上	同上	同上	同上	A	Mt2	D
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D		
12:58	同上	同上	同上	同上	同上	同上	同上	D	Mt3	A
13:00	b 50	c 100		D 100	250	3D 300	450	A		
13:30	b 50			D 100	150	3D 300	350	A		

(資源は平均使用CPU資源(MIPS)、DはDES-CBC、3Dは3DES-CBC、AはAES)

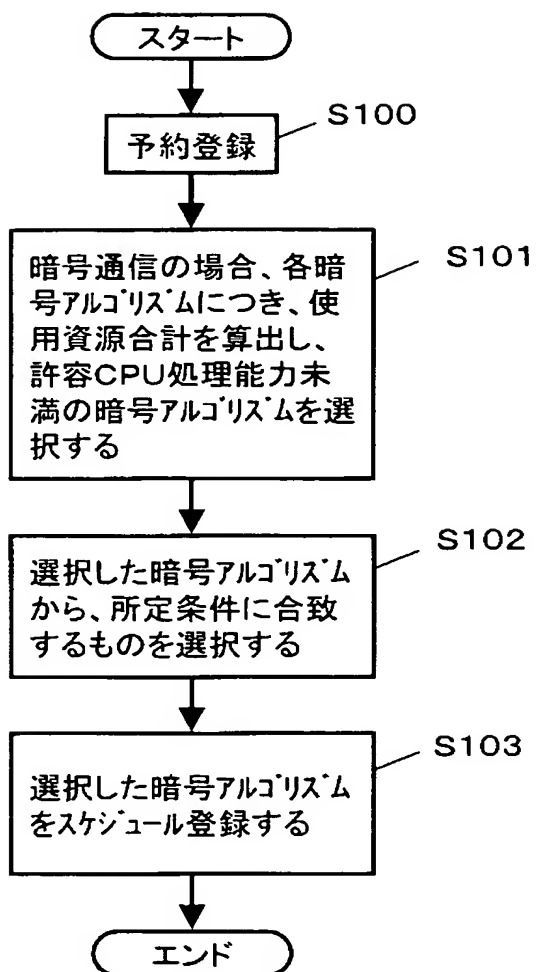
(2)暗号情報決定部の暗号処理使用資源表

暗号アルゴリズム	平均使用CPU資源(MIPS/Mbps)	平均使用メモリ資源(MB)	暗号強度順位
DES-CBC	100	13	3
3DES-CBC	300	20	2
AES	200	16	1

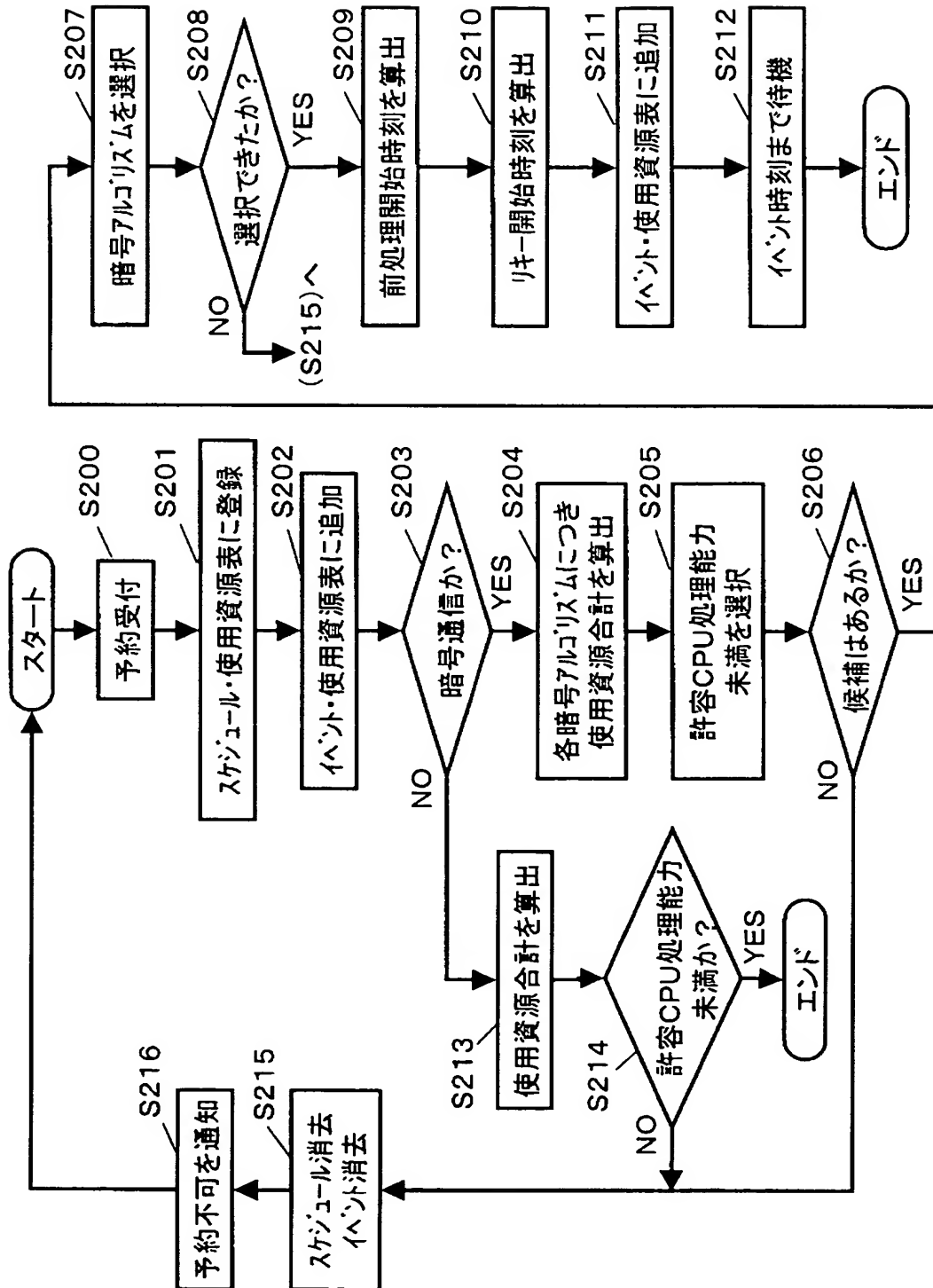
【図 9】



【図 10】

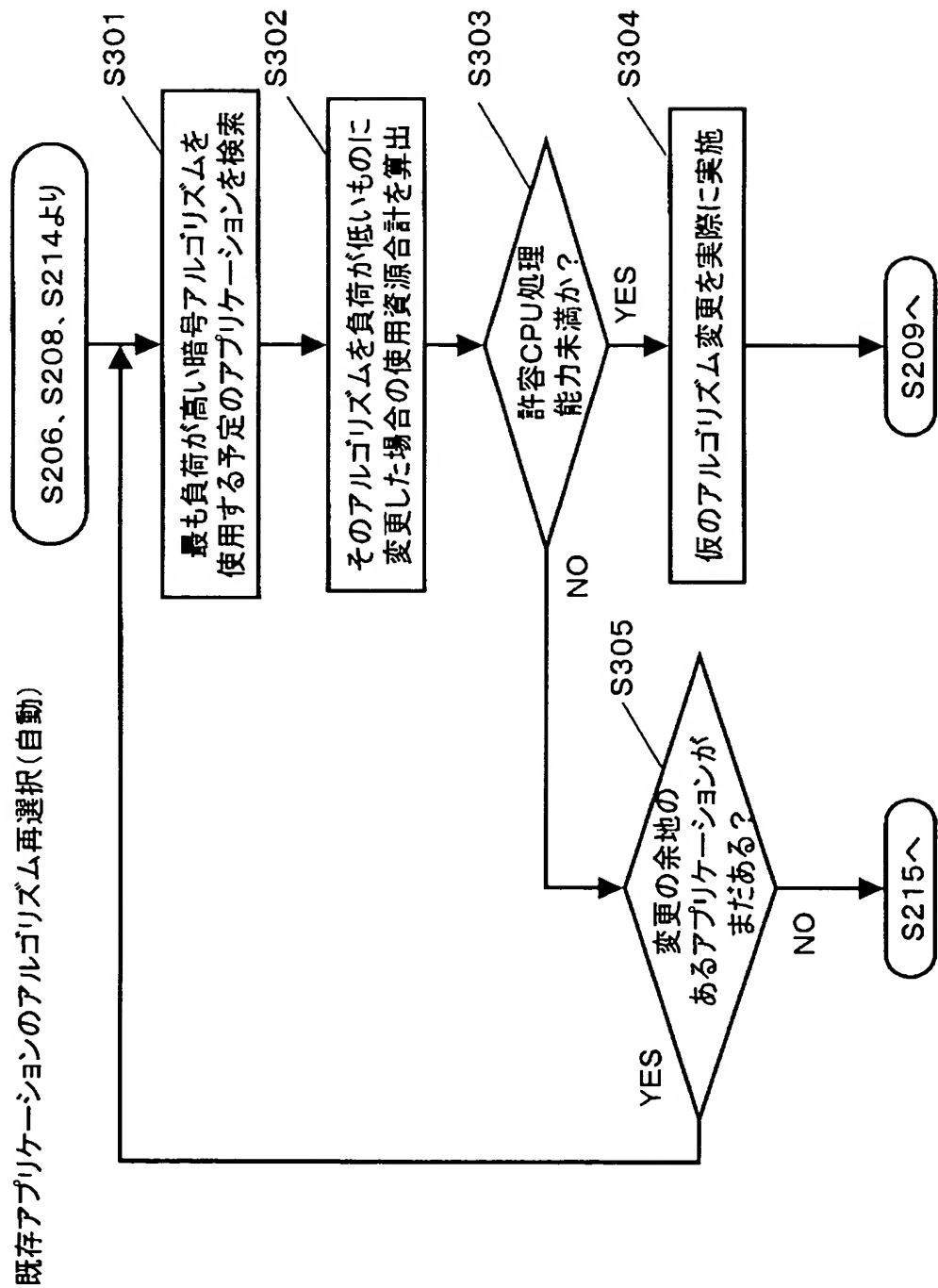


【図 11】

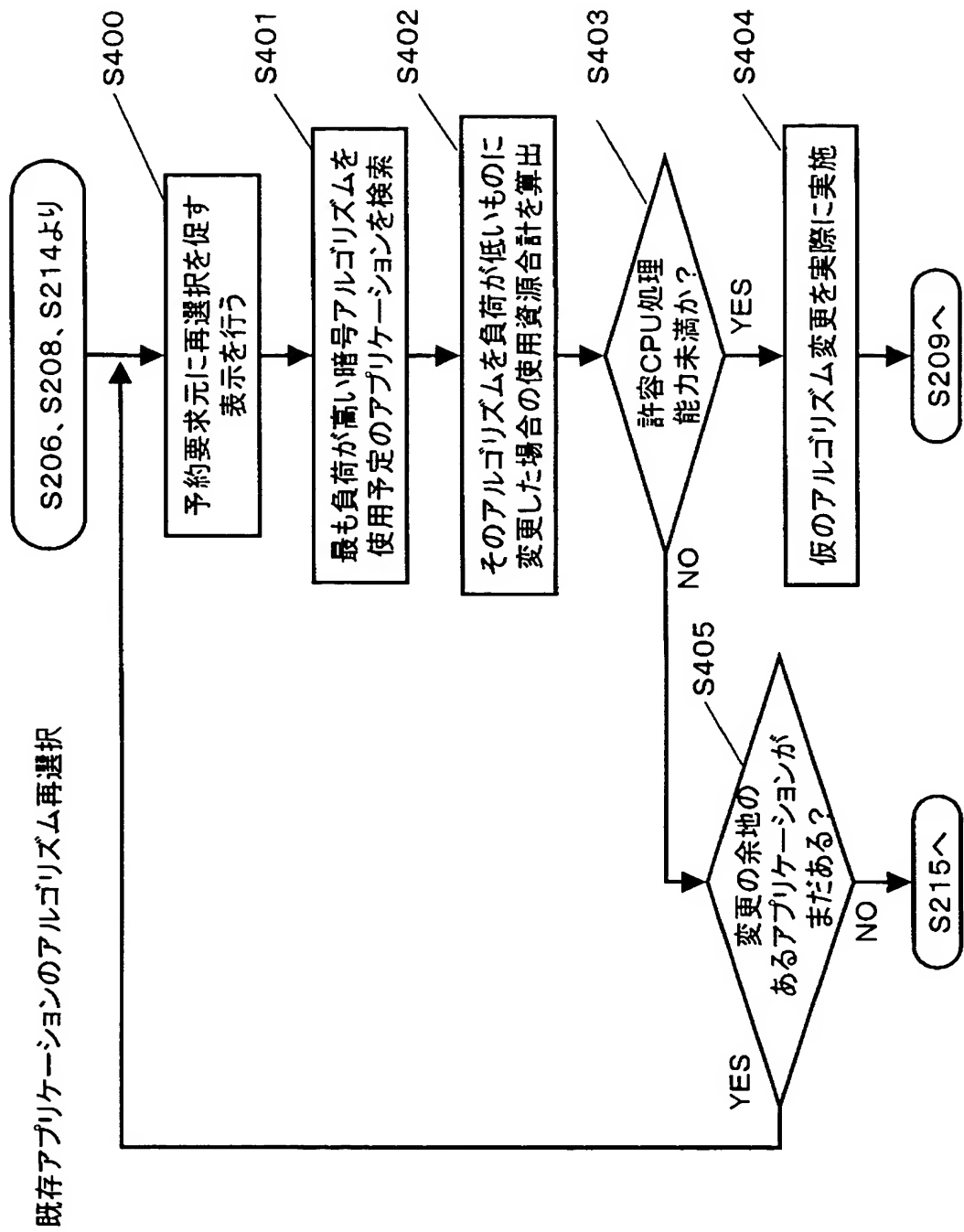




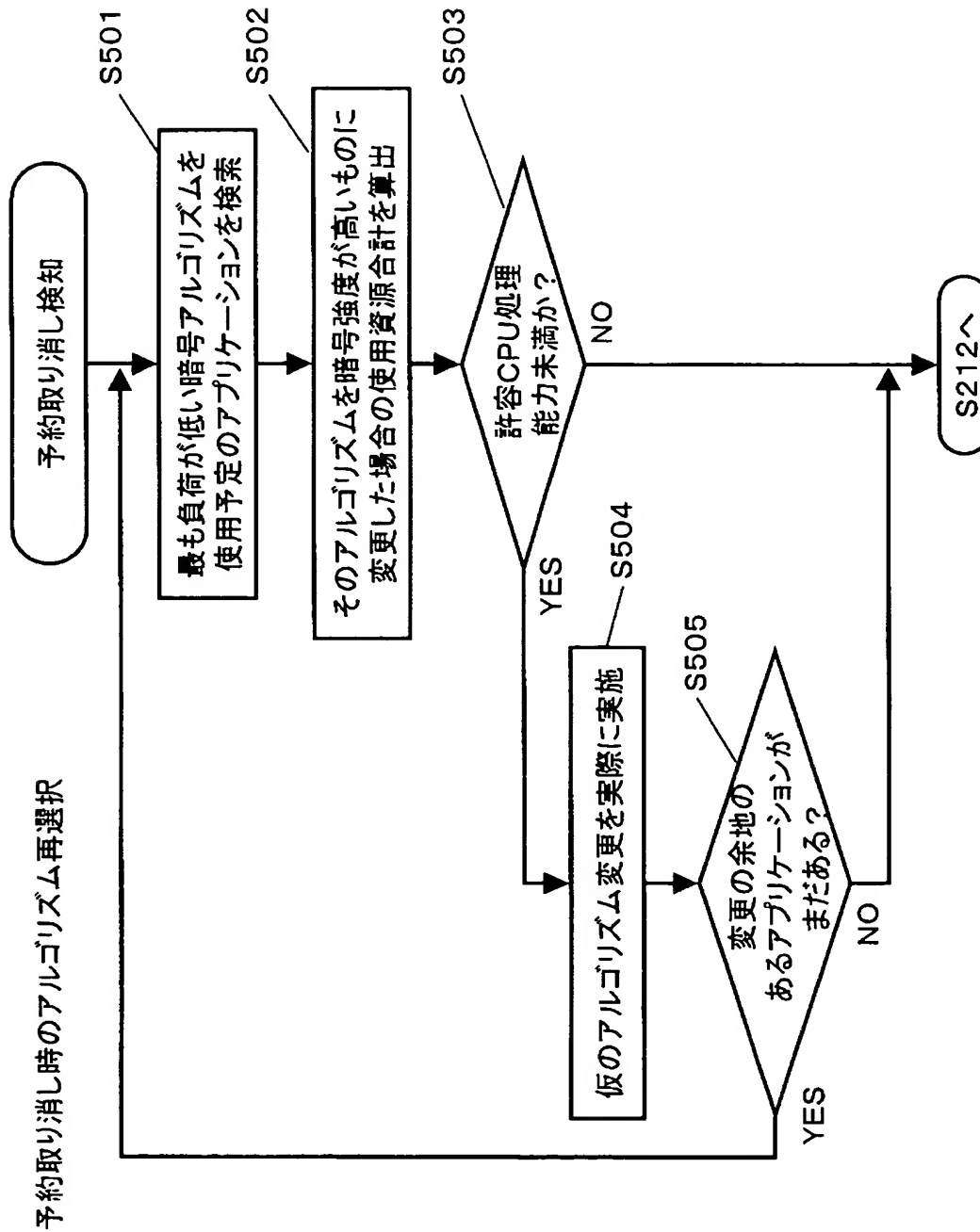
【図 12】



【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 暗号、認証などの処理と他の高負荷な処理を同時に行った場合、C P Uリソースが不足するという問題が起こり得る。例えば、ネットワークカメラなどの暗号通信処理と、T V録画などの高負荷な処理を同時に行った場合、どちらかの処理が正常に行えない場合がある。このような場合においても、両方の処理をリアルタイムに正常に行えるような、暗号アルゴリズムを選択する方法を提供する。

【解決手段】 複数種類の暗号アプリケーションが選択できる環境下において、予約されたアプリケーションや暗号通信アプリケーションの予約スケジュールと各アプリケーションや暗号アルゴリズムの消費するC P U処理能力などの資源の消費予想に基づき、使用する暗号アルゴリズムを選択してスケジュールする。

【選択図】 図 1

特願 2 0 0 3 - 0 2 3 7 9 7

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社